EXHIBIT 3

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION,
Plaintiff,
v.
SOLARWINDS CORP. and TIMOTHY G. BROWN,
Defendants.

) Civil Action No. 23-cv-9518-PAE

VIDEO RECORDED EXAMINATION OF
GREGORY RATTRAY
WEDNESDAY, FEBRUARY 12, 2025
NEW YORK, NEW YORK

CERTIFIED STENOGRAPHER:
JESSIE WAACK, RDR, CRR, CCRR, NYRCR, NYACR, CCR-NJ (No. 30XI008238700) CSR-TX (No. 11958) CCR-WA (No. 21007264), CSR-CA (No. 14420), REALTIME SYSTEMS ADMINISTRATOR
JOB NO. 250212JWAA

VIDEO RECORDED EXAMINATION of GREGORY RATTRAY, taken before JESSICA R. WAACK, Registered Professional Reporter, Registered Merit Reporter, Certified Realtime Reporter, Registered Diplomate Reporter, California Certified Realtime Reporter, New Jersey Certified Court Reporter (License No. 30XI008238700); Texas Certified Shorthand Reporter (License No. 11958); Washington State Certified Court Reporter (License No. 21007264); California Certified Shorthand Reporter (License No. 14420); New York Association Certified Reporter, New York Realtime Court Reporter and Notary Public of Washington, D.C. and the States of New York, Pennsylvania, Delaware, Maryland and Virginia, at Latham & Watkins, 1271 Avenue of the Americas, New York, New York, on Wednesday, February 12, 2025, commencing at 9:41 a.m. and concluding at 6:46 p.m.

A P P E A R A N C E S

ON BEHALF OF THE PLAINTIFF:
SECURITIES AND EXCHANGE COMMISSION
BY: CHRISTOPHER CARNEY, ESQ.
BY: JOHN TODOR, ESQ.
BY: CHRISTOPHER BRUCKMANN, ESQ.
BY: KRISTEN WARDEN, ESQ. (Remote)
BY: LORY STONE, ESQ. (Remote)
100 F Street, N.E.
Washington, D.C. 20549
PHONE: 800-732-0330
EMAIL: Carneyc@sec.gov

ON BEHALF OF THE DEFENDANTS:
LATHAM & WATKINS LLP
BY: SERRIN TURNER, ESQ.
BY: MATTHEW VALENTI, ESQ. (Remote)
1271 Avenue of the Americas
New York, New York 10020
PHONE: 212-906-1330
EMAIL: Serrin.turner@lw.com

A P P E A R A N C E S

ON BEHALF OF THE DEFENDANTS:
LATHAM & WATKINS LLP
BY: SEAN M. BERKOWITZ, ESQ.
BY: MAURICE BAYNARD, ESQ.
330 North Wabash Avenue, Suite 2800
Chicago, Illinois 60611
PHONE: 312-777-7016
EMAIL: Sean.berkowitz@lw.com

A L S O P R E S E N T
(REMOTE)
ANNIE GRAVELLE
BECKY MELTON

A L S O P R E S E N T

DANNY ORTEGA, videographer
ERIC COLE
ROZALIA (ROZI) KEPES

--o0o--

INDEX TO EXAMINATION
WITNESS: GREGORY RATTRAY

INDEXED PAGES

INFORMATION REQUESTED
None

WITNESS INSTRUCTED NOT TO ANSWER
None

INDEX TO EXHIBITS
WITNESS: GREGORY RATTRAY
Wednesday, February 12, 2025

INDEX TO EXHIBITS
WITNESS: GREGORY RATTRAY
Wednesday, February 12, 2025

INDEX TO EXHIBITS
WITNESS: GREGORY RATTRAY
Wednesday, February 12, 2025

** EXHIBITS BOUND SEPARATELY ***

--o0o--

******

PROCEEDINGS

February 12, 2025, 9:41 a.m.

New York, New York

******

THE VIDEOGRAPHER: We are now on the record.

My name's Danny Ortega, and I'm the legal videographer for Gradillas Reporting. Today's date is February 12, 2025, and the time is 9:41 a.m.

This video deposition is being held at 1271 Avenue of the Americas, New York, New York, in the matter of SEC vs. SolarWinds Corp., et al.

The deponent today is Gregory Rattray. All counsel will be noted on the stenographic record.

The court reporter today is Jessie Waack, and will now swear in the witness.

*****

GREGORY RATTRAY, sworn on oath and/or affirmed, called as a witness herein, was examined and testified as follows:

*****

///

EXAMINATION

BY MR. CARNEY:

Q. Good morning, Dr. Rattray.

A. Good morning.

Q. Just we haven't met before. My name's Chris Carney. I'm an attorney with the SEC.

Sir, you've had your deposition taken before, right?

A. Yes, I have.

Q. So I know you know the ground rules, but let me just walk through some of them really quickly.

So obviously our court reporter here is taking down everything we're saying, so it's important that we don't talk over each other. So even if you see where I'm going, just let me finish my question, and then you respond, and we'll have a clean record.

Is that okay?

A. Understood.

Q. And we'll take breaks from time to time, but if at any point you need a break, just let me know.

And the only thing I would ask is that if there's a question pending, that you just

answer the question, and then we can take the break.

And obviously the most important thing is that you're under oath the same as if you were in a court. So just give the answers truthfully to the best of your abilities.

Is that okay?

A. Yep, I understand.

Q. Okay. And is there anything that would prevent you from being able to testify fully and truthfully today?

A. No.

Q. All right. And were you retained to provide expert services in this case?

A. Yes, I was.

Q. And who are you retained by?

A. The -- Latham, the law firm.

Q. Okay. And so you were hired directly by Latham & Watkins?

A. Actually, Serrin, you know, I --

THE WITNESS: I believe we were hired by Latham, right?

You know, I don't know if the contractual relationship is with SolarWinds directly.

BY MR. CARNEY:

Q. Okay. All right. When you get paid, is it Latham & Watkins that pays you?

A. Again, my team invoices, and I get paid. So I'm actually not exactly sure --

MR. TURNER: I can represent that SolarWinds pays the invoices.

THE WITNESS: SolarWinds.

BY MR. CARNEY:

Q. And do you know how much you've been paid so far in this case?

A. I don't know the total amount.

Q. Okay. Do you know how many hours you personally have spent on this case?

A. I would say 200-ish, yeah.

Q. All right. And for purposes of this case, what do you consider your area of expertise to be?

A. My area of expertise relevant to this case is, you know, understanding how companies, enterprises control their information environment, implement security controls.

Q. Okay. And is there a field of expertise that you would fold that into?

A. You know, different labels are used,

but information security or cybersecurity.
Q. Okay. And do you consider yourself an expert in cybersecurity?
A. Yes, I do.
Q. Okay. You don't hold a degree in computer science, do you?
A. I hold a bachelor of science, but I don't hold a computer science degree.
Q. And a bachelor of science in political science and military history, right?
A. Yes, I do.
Q. And have you taken any courses in computer engineering?
A. I've taken courses in technology policy. I haven't taken any -- any university courses in computer science or engineering.
Q. And your master's degree, as I understand, is in public policy; is that right?
A. That's correct.
Q. And you have a PhD in international security; is that correct?
A. That's where I wrote -- at Tufts University where I wrote my dissertation on the future of cyber warfare.
Q. And that was at the Fletcher School?

A. That's correct.
Q. And as I understand it, at the Fletcher School a PhD in international security is a concentration within the international relations PhD program; is that right?
A. The Fletcher School is the Fletcher School of Law and Diplomacy. There's actually not -- you know, there's not a specific concentration inside the school for the PhD program. You know, you have to have areas of study. One of mine was technology policy.
Q. Okay. And did your PhD course or program at Fletcher require any computer science courses?
A. No computer science courses.
Q. Did your PhD program require any courses in information security to complete the degree?
A. I did research courses, sort of guided research courses with professors around the evolution of at that time a fairly nascent computer and information security, but there was no -- there was no formal course in information security.
I'm not sure that such courses existed

at the time.
Q. Can you remind me what year you received your PhD?
A. 1998.
Q. Did your PhD program require any courses in software security to complete the degree?
A. No.
Q. Did your PhD program require any courses in computer network security to complete the degree?
A. No, it did not.
Q. Have you ever taken a course in software security?
A. I have not taken a course in software security.
Q. Okay. Have you ever taken a course in computer network security?
A. Again, I've done a lot of guided research by professors in the technology field that included, you know, information technology, computer technology, security controls, but it wasn't a formal course. It was a formal course in the sense that I got credit.
It wasn't a, you know, predesigned

course. It was an independent-guided research course.
Q. Okay. Did your PhD program require any courses in applied cryptography?
A. No.
Q. Okay. And have you taken any courses in applied cryptography?
A. No.
Q. All right. Have you personally designed any cybersecurity systems?
MR. TURNER: Object to the form of the question.
THE WITNESS: I designed quite a few cybersecurity systems in terms of programs that companies run. You know, red team operations and processes, vulnerability assessment, you know, processes, you know.
So everything from major organizations, information security, you know, approaches to certain types of operations that take place inside those programs, I've designed those processes and programs.
BY MR. CARNEY:
Q. And you mentioned you did this for companies.

Which companies did you design these cybersecurity systems for?
A. I designed the cybersecurity program for JPMorganChase while I was the CISO. I helped with the formulation of the nation cybersecurity strategy when I was at the White House and then, you know, at while -- in two different commands in cybersecurity in the Air Force.
Designed different programs including, you know, the Air Force's red team and penetration testing program.
As a consultant, I've helped companies design their programs both overall cybersecurity programs and specific threat intelligence and red team and penetration testing programs.
Q. Okay. And when you were -- let's use JPMorgan for an example. That was the first one you mentioned.
When you designed their cybersecurity program, were you responsible for any of the technical implementation of that program?
MR. TURNER: Object to form.
THE WITNESS: I was, as the CISO, responsible for the oversight of the entire

program including its technical implementation.
BY MR. CARNEY:
Q. Did you do any of the actual coding involved in creating the cybersecurity controls?
A. You know, I did not do any coding. The control structures included both technical and, you know, nontechnical controls. You know, the program as a whole, you know -- yeah, I work -- design -- was responsible for the design and oversight of the entire program.
Q. Okay. With respect to you mentioned technical controls, do you have the capability yourself to code technical controls?
MR. TURNER: Object to form.
THE WITNESS: Technical controls often don't involve coding, so I'm not a coder.
BY MR. CARNEY:
Q. Okay. What do they involve then if they don't involve coding?
A. You know, many involve -- if we're talking about -- are we talking about technical controls?
Q. Yes, technical controls. Thank you, sir.
A. In a technical control such as network

monitoring, you're often using tools that are in place on devices and networks to, you know, monitor whether -- you know, whether these things occurred.
Q. And do you -- how are those tools created?
MR. TURNER: Object to form.
THE WITNESS: You know, the tools are created initially through coding, though the point at which enterprises use them, they're usually not -- there's no coding involved with the tools at the point at which an enterprise deploys the tools.
BY MR. CARNEY:
Q. Okay. And do you have the technical skills and capability to deploy those tools yourself?
MR. TURNER: Object to form.
THE WITNESS: There's a wide variety of tools. Some of them are pretty simple. I'm not a hands-on technologist.
So, you know, the ones that are relatively straightforward for a user to deploy, I can deploy.
///

BY MR. CARNEY:
Q. What about the tools that are deployed at an enterprise level? Do you have the skill set to be able to do that?
MR. TURNER: Object to form.
THE WITNESS: I think we'd have to get a little more specific as to -- you know, again, relatively simple, you know, user level tools are deployed in an enterprise, and then there's more sophisticated -- you know, there's more complicated tools deployed.
BY MR. CARNEY:
Q. Well, I think you -- the example you gave was network monitoring tools.
Do you -- would you have the technical capability to deploy network monitoring tools at an enterprise level for, say, JPMorgan?
A. No, I would not.
Q. Okay. And what kind of skills would someone need to have to do that?
A. So we're talking about the skills necessary to deploy a network monitoring system?
Q. Yes, Doctor.
A. And just deploy it, right? Are we talking separate from the operation of that --

Q. Just to deploy it.
A. Yeah. You know, it would basically be, you know, experience in software deployment, which is usually residual in the -- you know, the architecture or infrastructure teams in a large enterprise.
Q. Okay. Do you hold any cybersecurity certifications?
A. Defining "certification" as -- can we just get a definition of what we mean by "certification"?
Q. Well, I'll give you an example.
Are you familiar with CompTIA, and that's C-o-m-p-T-I-A?
A. Yes, I am.
Q. And they offer cybersecurity certifications, right?
A. Yes, they do.
Q. And do you hold any of those?
A. I do not.
Q. Are you familiar with -- and this is all caps I-S-C 2, which is the International Information Systems Security Certification Consortium?
A. Yes, I am.

Q. And what is ISC2?
A. It's a number -- one of a number of different bodies in the -- in the cybersecurity field that, you know, works to train and certify people.
Q. Okay. And ISC2 offers cybersecurity certifications, right?
A. I believe they do.
Q. And do you hold any of those?
A. I do not.
Q. And do you have -- I'll spell it out -- C-I-S-S-P certification?
A. I do not.
Q. Do you have any -- do you have any SANS GSEC certification?
A. I'm not sure what those certifications are. I don't hold them.
Q. And are you familiar with CertNexus, and that's C-e-r-t and then capital N-e-x-u-s?
A. I don't believe I am.
Q. And, Doctor, you're aware that this litigation involves SolarWinds's security statement, right?
A. Yes, I am.
Q. And before reading SolarWinds's

security statement for this litigation, had you ever read other company's security statements?
A. Yes, I have.
Q. And in what context? Why had you done that?
A. Both in the context of, you know, I guess, you know, I want to make sure that we're talking -- when you say "a security statement," you know, we might want to define that a little bit.
If it's about public declarations of the company's security posture, you know, I just want to make sure that's the frame we're putting on it as the answer to the question.
Q. Sure, sure.
So I'm talking now about the SolarWinds's public-facing --
A. Yep.
Q. -- security statement that's at issue in this case --
A. Yes.
Q. -- as well. I'm asking about analogous security statements at other companies.
A. Yes, I've seen them. You know, at JPMorgan, when I was a CISO there, we made --

that's why I wanted to clarify.
We made public statements about our security that I don't think we put it in the form of a security statement like we see at SolarWinds.
I've also seen them in consulting, you know, engagements that I've had, you know, much more similar to the SolarWinds situation.
Q. Okay. And let me break that down.
So have you ever written the public-facing securities statement of an organization?
A. I have been involved in the -- you know, the creation, the establishment of, again, public-facing security statements.
Again, I guess the question is, how close to the -- you know, how much am I looking at exactly the type of statement that SolarWinds had.
But I've been -- I've certainly been involved in the creation of public-facing statements about security. You know, I think that's -- we can refine if necessary.
Q. Sure. And about how many companies have you done that for?
A. Again -- well, it probably gets to the idea that the way securities statements are, you

know, established publicly usually is not an individual, you know, activity, and it wasn't in the case of SolarWinds, right?

I've been involved in processes where companies are deliberating about what to say about their security posture, commenting on draft language, drafting language at times.

Q. Okay. And are there specific companies you can recall doing that for?

A. You know, again, certainly with JPMorgan when we were making public statements about security, I was involved in those.

And in consulting work, I, you know, basically am under nondisclosure agreements about the specifics of activities I undertook.

When I was the chief security advisor to ICANN Internet Corporation For Assigned Names and Numbers, we made -- you know, we made -- we may have made statements. I don't remember exactly, so I probably was involved during the period I was there.

Q. Okay. And have you ever in your work had to advise -- forgive me if this covers what you already said.

But have you ever been called upon to

description of practices, I've done that over and over again, yes.

Q. And have you ever had to advise a company to modify its security statement, because their practices didn't match what the security statement said?

A. You know, I'm just -- I'm seeking to recall. I think -- you know, I can't recall a specific instance of modifying language related to a public-facing statement.

Again, are we -- are we good with you saying security statement, and me thinking about this more broadly as, you know, public statements made by companies related to their security? Are we saying the same thing?

Q. Yeah, I think we're saying the same thing.

A. Okay.

Q. All right. Let me delve in a little bit in your expertise in cybersecurity.

And if it helps -- I'm going to hand it to you in a little bit. I have your CV here. So if you need it, let me know.

But where in your background do you have expertise in access control?

advise a company on their security statement that they were writing?

A. Again, you know, a lot of times they're not called security statements, you know, sort of -- but I have advised on the establishment of public-facing security language for companies.

Q. Have you ever, in your work prior to this case, had to analyze the security statement of an organization to see if it matched what they were actually doing?

A. I've conducted numerous assessments of companies, cybersecurity postures, control structures. That has informed in the cases where I've been consulting my opinion about, you know, things that they're going to say publicly. You know, I would say that would be the way to characterize my experience.

Q. Okay. Have you ever taken a public-facing security statement and analyzed whether what the company was doing matched what they said in that public-facing security statement?

A. You know, to the extent that which security statements, you know, describe control structures and you assess, you know, you know,

A. You know, starting in my military career, you know, as we started to define, you know, what we initially called information warfare and then called cybersecurity cyber warfare, you know, I was involved, you know, in the development of approaches both -- you know, both policy and procedural.

But also operational related to, you know, how Air Force organizations, you know, would need to implement that.

And then as commander of two separate Air Force organizations, which in these cases were cybersecurity organizations, we -- we were required to implement the information security practices of the Air Force as commander and, therefore, had oversight of an information security program which had detailed access control provisions.

One of those organizations also wrote the first set of what we call tactics, techniques and procedures for cybersecurity, which would have -- you know, which did include, you know, the full set of things that an organization should perform while the -- defending their networks, which would include access controls. So that

probably describes my Air Force experience.
As, you know -- as a consultant, you know, in conduct of -- you know, information security assessments of organizations, I have led and reviewed assessment reports about the presence of access controls in a large number of organizations.
In the JPMorgan role, we had -- access controls were, you know, part of the broader information security program where we had policies and procedures.
I reviewed those policies and procedures as well as, you know, had metrics provided to me about the implementation of our policies and procedures. I think that's a fairly comprehensive review.
MR. TURNER: I just want to flag for the court reporter, it's "tactics, techniques and procedures."
BY MR. CARNEY:
Q. All right. So thank you for that.
In addition reviewing the policies and procedures and receiving metrics on the implementation of those policies and procedures, do you have any sort of technical skills or acumen

as it relates to designing access controls?
MR. TURNER: Object to form.
THE WITNESS: You know, I've been involved in, you know, deciding, you know, how strong certain access controls, things like, you know, password complexity and how hard should we make it or provisions for -- in a data loss prevention systems, you know, what are the things that would be flagged down to the implementation level of those systems in terms of what would be present in the implementations of those systems.
Again, I'm not a coder, so I did not go down to the coding level in my experience with the implementation of security controls.
BY MR. CARNEY:
Q. Okay. What is -- what about the sort of same question as it relates to user identification?
What's your experience as it relates to user identification?
A. You know, both as a user in many organizations -- we can go through them, but I don't think we need to, you know, in the different sort of organizations I've been involved with over the years.

You know, similar to password, you know -- the implementation of password controls, user identification is usually an element in most, you know -- some policy and procedure approaches around naming conventions for users on a network.
So I've certainly been involved in the development of, you know, user access controls and agreements, which, you know, specify the level of, you know -- like, how people will be identified in a user identification system.
I'd say that probably characterizes my experience.
Q. And similar to my earlier question, do you have any sort of technical skills as it relates to implementing user identification requirements?
MR. TURNER: Object, again, to form. "Technical."
THE WITNESS: Right. The implementation of user identification systems is not a particularly technical activity, you know, in terms of it's mostly a process, you know, setting activity.
And, again, I've described and I can repeat if you like, sort of my, you know, my

experience in the process setting side of things.
You know, the tools are, you know, developed and deployed as we've already discussed.
But, you know, at an enterprise level, it's almost all a decision about the processes you develop and deploy on those tools in order to achieve a security control, which, again, I've been involved pretty directly in that.
BY MR. CARNEY:
Q. Okay. Have you -- do you have any involvement or experience in developing software?
MR. TURNER: Object to form.
THE WITNESS: I have certainly, you know, overseen programs that are, you know, responsible for ensuring the security and the development of software.
I'm not a coder, so, you know, if the question is, do I do coding, I don't do coding.
BY MR. CARNEY:
Q. And so what was your responsibility for ensuring the security in the development of software?
A. Oversight of and then consulting on secure software development, you know, procedures in -- you know, in the development environment in

different countries -- not countries -- companies.
Q. And what different companies were you involved in the secure development lifecycle process?
A. At JPMorgan, we had a secure development, you know, emphasis -- right? -- you know, inside the security programming in conjunction with the application developers in the company.
I -- you know, in consulting reviews, you know, again, secure development is an element of most security reviews at this stage, so I've been involved in sort of numerous reviews and assessments of secure development environments.
Q. And what -- what kind of software was JPMorgan developing that used the -- can I call it SDL process?
A. Yeah, call it -- yeah, we'll use SDL.
You know, JPMorgan develops a wide variety of applications for both, you know, internal use and external, you know, use by customers. You know, very large numbers of different applications was -- this process was -- was part of.
Q. And when you were the CISO at

JPMorgan, you had some involvement in that process?
A. I had oversight of the, you know -- in, you know, review of the processes we had asked the technology teams to implement.
Q. The SDL process that JPMorgan followed, was that -- you know, was that based on the Microsoft SDL process?
A. I'm not at liberty to get into sort of any specifics because of my exit agreement with JPMorgan about specifics inside the JPMorgan security program.
Q. Okay. Have you ever personally conducted threat modeling?
A. Many times. In basically the idea that a security program, a -- you know, the development of technology for a company needs to take into account, you know, threat-based risks, you know.
You know, I've been the -- many person identifying threats to organizations, you know, at the organizational, even the national level in terms of, you know, how -- who are threat actors?
How do they behave? How do they pose risk to companies? Are the control structures in

the company -- you know, attune to that?
Are we feeding our knowledge of how threat actors behave into, you know, processes like software development. So I have a lot of experience with, you know, threat modeling.
Q. So as an expert in cybersecurity, how would you define threat modeling?
A. You know, in practice, and, again, across a wide variety of organizations and experiences, threat modeling is, you know, used fairly broadly to describe, you know, how a -- a sort of process or a callout to, you know, look at risks that, in particularly security risks or cybersecurity threats and, you know, understand how that is affecting, you know, the security process you're either implementing or the project that you've got underway.
That's how I think about threat modeling.
Q. And I know from your report, you're familiar with NIST, right?
A. The National Institute of Standards and Technology?
Q. Yes.
A. Yes, I am.

Q. And you're familiar with ISO?
A. The institute, the International Standards Organization. Yeah, I'm aware of both of those organizations.
Q. And are you familiar with those organizations' specific threat model structures that they have put out?
A. I've not yet -- I don't know that either organization's put out any threat modeling. They may have, right? I'm more familiar with cybersecurity frameworks that they've, you know, put out.
Q. And I guess what I'm trying to understand is that the way you describe threat modeling, you don't think of it necessarily as a specific set of defined activities; is that fair to say?
A. That's fair. I mean, there's -- a lot of people do it a lot of different ways, in my experience.
Q. And if a company was performing threat modeling, what sort of evidence would you expect to see?
A. I mean, you know, one would want to see, you know, evidence that they were considering

threats that security concerns were baked into, you know, development processes for technology that were, you know, being considered that, again -- you know, the notion that threat-based risks were being considered as, you know -- you know, and then incorporated in the activities that were being -- you know, were underway.

That's how I think about, you know, both threat modeling and, you know, what you would be looking for in order to evidence the presence of it.

Q. And you've touched on a bit your experience with cybersecurity assessments.

Have you ever had an experience in which an organization was not following some of the cybersecurity policies that it professed to follow?

A. You know, in general -- in general, when one does an assessment, it's not a binary sort of determination of, you know, follow versus not follow.

It's, you know -- you know, an assessment of the full set of procedures, understanding evidence that you have available to you.

You know, talking with, you know, people in the company as well as if others have assessed the same sort of, you know, either program or process and, you know, determining, you know, the degree of which, you know, in an assessment, you know, that -- if we're looking at a control or a control structure, that, you know, that's in place in its maturity.

Q. Just hypothetically, you've never had a situation where a company said, we follow such and such password policy, and then you went in, looked under the hood, and they weren't actually following that policy?

A. I'm just trying to think of -- you know, I definitely had instances where, you know, you see a, you know, small number of violations in a large organization, right?

I mean, that's natural, and it's actually good that you're doing an assessment in order to determine, you know, whether the implementation all the way down to humans who make errors are doing things in a -- you know, in a situation.

You know, it is very rare, and I'm trying to, you know, rack my brain to see that an

organization that said it had a policy is just fundamentally absent in the performance of that.

Because, again, it's a -- sort of a gradation from, you know, the presence of the call-out to do something to how much is it being done, right? You know, either more or less.

Q. Okay. And I just want to back up a second to -- before we get too far away from it.

You had talked about -- when I asked you whether you personally conducted threat modeling, and you said that you had done it many times basically in the idea that in a security program, you need to take into account threat-based risks and identify threats to organizations and threat actors.

And I'm just wondering, the sort of steps that you listed that you've personally done, would you consider these to be standard steps of threat modeling in the cybersecurity field?

A. You know, I don't think there's a standard in this area. This area in particular is one of those where the concept is there, but people execute it in very different ways.

So, you know, I don't -- in my opinion, there's not a standard approach to doing

this. There's a call-out to do it.

Q. There's a couple -- we'll get to your report in a second. I promise. But there's a couple instances in your report were you mention SOX -- and that's all caps S-O-X --

A. Yeah.

Q. -- audits.

Do you personally have any experience with SOX audits?

MR. TURNER: Object to form.

You're asking whether he's done them or had experience.

MR. CARNEY: Involvement whether he's done them; involvement, any sort of experience with them.

THE WITNESS: Yes. I -- you know, again, broadly defined in terms of experience, I've been, you know, in organizations including JPMorgan that have undergone SOX audits.

And I've, you know, reviewed them many times often as part of assessment processes, you know, in companies just to take a look at what the SOX audits show about -- you know, my focus has generally been information security controls.

///

BY MR. CARNEY:
Q. In conjunction with the SOX audits, have you had to make any determinations as to whether particular controls related to financially material systems?
A. I have not --
MR. TURNER: Object to form.
THE WITNESS: Okay.
I have not been an auditor, so I haven't, you know, made SOX audit determinations. You know, again, I haven't played the auditor role.
BY MR. CARNEY:
Q. Okay. Have you had any experience within -- and this is capital S-O-C 2 audits?
A. Yes. Pretty much similar experiences. You know, JPMorgan underwent SOC 2 audits. I've seen a lot of SOC 2 auditing reports in consulting engagements just in terms of, you know, what SOC 2 auditors have said about control structures and in organizations I've worked with.
Q. All right.
(Whereupon, Exhibit 1 is marked for identification.)
///

(Whereupon, Exhibit 2 is marked for identification.)
MR. CARNEY: The shorter one is Number 1. The bigger one is Number 2. Here's Number 2. I might have another copy if you...
MR. TURNER: No, that's fine. I've seen it before.
THE WITNESS: I assume I'm not allowed to write on these?
MR. TURNER: I'm just going to put the exhibit number on them.
THE WITNESS: Okay.
BY MR. CARNEY:
Q. All right. Dr. Rattray, I've handed you what the court reporter has marked as Rattray Exhibits 1 and 2.
A. Uh-huh.
Q. And just for the record, Exhibit 1 -- and you can confirm this for me -- if you look at the back, the last page, it should have a December 30, 2024, date; is that right?
A. The last page of the main report?
Q. The last page of the entire document.
A. Oh, the entire document?
Q. Yeah.

A. Yes.
Q. Okay.
A. Yes, December 30, 2024.
Q. Right.
A. Yeah.
Q. And so this was a corrected report, if you will, that made some sort of minor typographical corrections to your earlier report; is that right?
A. That's what I remember as well.
Q. Okay. And so unfortunately, that report didn't have the same appendices to it, so I've handed you what's been marked as Exhibit 2, which has your appendices with your documents reviewed, your CV and your prior testimony.
MR. TURNER: We would have been happy to attach the same attachments, for the future. Happy to send you something like that.
MR. CARNEY: Not a big deal.
MR. TURNER: Okay.
MR. CARNEY: There's no...
MR. TURNER: Killed a few trees in the process.
MR. CARNEY: Yeah.
///

BY MR. CARNEY:
Q. So is it fair to say then, to Mr. Turner's point, that the appendices in your original report from November would be the same appendices that would be attached to Exhibit 1?
A. Yeah, as I remember reviewing the minor revisions, I didn't see anything when I reviewed them that would have indicated a change in any of the attachments from the original report.
Q. Okay. Great.
So let's focus on Exhibit 1 for the moment.
Have you finished all the work that you were assigned to do in this case?
A. You know, I believe I have the right if I receive new evidence to augment. I don't have any current plans to do so.
Q. Okay. Did you yourself write Exhibit 1, your expert report?
MR. TURNER: Object to form.
THE WITNESS: I wrote the report. And, you know, with the -- you know, with the assistance and, you know, collaboration with the law firm, Latham -- Latham & Watkins.

BY MR. CARNEY:
Q. And aside from Latham & Watkins, did anyone else help you write your report?
A. I had research assistants from -- analysts from my consulting firm, but they did not write any of the report.
Q. And who were those research assistants?
A. Helen Lee.
Q. Okay. And do you know what Ms. Lee's background is?
A. I do.
Q. And what is it?
A. She's a graduate of Columbia University, and it -- has a master's degree with a focus on cybersecurity from the School of International and Public Affairs and has been an employee in my consulting group Next Peak.
Q. So she's an employee of Next Peak?
A. Yes.
Q. And besides Ms. Lee, did anyone else help you?
A. No.
Q. Okay. Did anyone from SolarWinds help you write this report?

A. No.
Q. I don't want you to tell me the substance of it. Your communications with counsel are covered by the work product, Rule 26.
But did you -- did counsel provide comments to you on your drafts of this report?
A. Yes.
Q. And did you incorporate some of those comments?
MR. TURNER: I'm just going to object to the questions in terms of starting to get into the details of the drafting process.
MR. CARNEY: Okay.
BY MR. CARNEY:
Q. I don't want to get into the details of the drafting process. But I'm just trying to understand how this came about.
Did -- you're familiar with Tim Brown, right?
A. I am.
Q. Did he provide any comments or suggestions to your draft reports?
A. I had one conversation with Tim about specifics on how, you know, his practice reviewed logging data. He did not comment on the report.

Q. And when you say "logging data," is that related to access controls?
A. It may be related -- we should look at the specifics.
Q. Okay.
A. You know, it may be access controls. It may be, you know, firewall -- the use of firewall. But we can look into the specifics in the report.
Q. Okay. And are all of the opinions you're offering in this case set forth in this report, Exhibit 1?
A. You know, as of today, yes.
Q. And as of today, you said, I think, you don't plan to offer any additional opinions?
A. That's --
MR. TURNER: Objection.
(Pause in testimony.)
THE STENOGRAPHER: I don't have a full answer.
THE WITNESS: You know, as I answered previously, I don't have any current plans to revise this report.
BY MR. CARNEY:
Q. Okay. And if you could just briefly

look at Exhibit 2. And, actually, it might be helpful that we have it as two separate exhibits, because you can look at them side by side.
If you look at Appendix A to Exhibit 2, is that a copy of your CV?
A. Yes, it is.
Q. And is this -- I'm not going to ask you to review the whole thing, but as far as you know it, does this accurately reflect your education and experience?
A. I believe it does.
Q. And you've served as an expert in a couple other cases; is that right?
A. That's correct.
Q. And how many -- was it two?
A. It's two, yeah.
Q. Okay. And has your expert testimony ever been excluded in whole or in part by a Court?
A. No.
Q. Has the Court ever imposed any kind of limitations on your ability to offer your expert opinions?
A. No.
Q. In the course of serving as an expert witness, has opponent ever filed a Daubert motion

against you?
A. Not to my knowledge.
Q. And we talked a little bit about your -- you know, your arrangement here, but can you just describe to me how did you become -- come to be retained as an expert in this case? Who contacted you?
THE WITNESS: I believe, Serrin, it was you. But it was definitely from Latham & Watkins.
BY MR. CARNEY:
Q. And had you ever worked with Mr. Turner before this case?
A. I had not.
Q. And do you know how he got your name or who referred you to him?
A. I don't know how he got my name.
Q. Man of mystery.
A. I mean, again --
Q. Yeah.
A. -- I don't know.
MR. TURNER: He has a reputation in this space. What can I tell you?
MR. CARNEY: All right.
///

BY MR. CARNEY:
Q. Okay. Prior to your retention, did you know anything about the SEC's case against SolarWinds?
A. Yes. I was aware that -- I'm trying to remember if the case had been filed, but I was aware that there was, you know, activity between the SEC and SolarWinds.
Q. Okay. Did you recall when you were retained on this case?
A. I believe it was about October -- I don't want to be held to the month -- of 2023.
MR. TURNER: Chris, whenever you have a moment, we've been going for about an hour. Take a break.
MR. CARNEY: Sure. We can take a break now. Want to take?
MR. TURNER: Yeah, thanks.
MR. CARNEY: 10 minutes?
THE VIDEOGRAPHER: The time right now is 10:32 a.m.
We are off the record.
(Whereupon, a recess was taken at 10:32 a.m.)
THE VIDEOGRAPHER: The time right now

is 10:44 a.m.
We're back on the record.
BY MR. CARNEY:
Q. Okay. Dr. Rattray, before we broke, you had mentioned that you had some familiarity with the SEC's case against SolarWinds before you became personally involved in the case; is that right?
A. That's right.
Q. And how did you acquire that knowledge?
A. You know, in my field, you know, in what I do, you know, you're reading news related to cybersecurity.
So the SEC action, and I forget the sort of specific legal terminology around the action, but sort of the original, you know, publicly known investigation, you know, I was just reading reporting on that.
Q. Okay. And were you familiar with what was known as the Sunburst incident?
A. Yes, I am. Yes, I am.
Q. Okay. And did you write any articles on that, do you recall?
A. No. I did not, that I can recall.

Q. And I'll remind you this: When I'm asking you this question, I understand you're not a lawyer. I'm not asking you for legal opinions or conclusions, but what is your understanding as to the basis of the SEC's case against SolarWinds and Tim Brown, as we sit here today?
MR. TURNER: Object to form.
THE WITNESS: You know, again, with your disclaimer, like, I'm not a lawyer and, you know, I'm not trying to offer legal opinion, you know, my understanding is the SEC is asserting that, you know -- assertions in the security statement are potentially fraudulent, because SolarWinds and Tim Brown, you know, knew that the state of their security was not -- not in line with what was, you know, said in the security statement.
BY MR. CARNEY:
Q. Okay. And once again, setting aside legal requirements, as a cybersecurity professional, do you believe it's important for companies and individuals to be truthful when making statements about their cybersecurity practices?
A. Yes, I do.

Q. And why do you believe that?
A. You know, in general, you know, cybersecurity is a complex, challenging field. And, you know, in -- our ability to pursue it, you know, needs to be based on, you know, good information that we need to trust that when we're communicating with each other, that, you know, to the best of an individual's, you know, ability, that they're representing things accurately.
Q. And if I could ask you, sir, to turn to paragraph 13 of Exhibit 1.
And you can read that whole paragraph to yourself if you want, but --
A. Oh, sorry. I turned to page 13.
Q. I'm sorry. Page 5, paragraph 13.
MR. TURNER: Which one are we on? Exhibit 1 or Exhibit 2?
MR. CARNEY: Exhibit 1. Thank you.
THE WITNESS: Yes. I've read it.
BY MR. CARNEY:
Q. And in the third sentence, you say, "I understand that the Securities & Exchange Commission (SEC) has alleged that these representations were false or misleading during the time period from SolarWinds's initial public

offering which occurred on October 19, 2018, to January 12, 2021."
And you refer to that as the relevant period.
Once again, not asking for a legal opinion, but what is your understanding as to what it means for a representation to be false or misleading as you use that term in this sentence?
A. Yeah, I'm not quite sure how I can -- you know, I could reframe words, but to me, those are pretty -- you know, do you want me to define what's a falsehood?
Q. And fair question. I'm just trying to understand your use of the term, so let me give you a -- try to give you a hypothetical. And once again, this is a hypothetical. I'm not saying this is SolarWinds's here.
But let's say you refer to a time period October of 2018 to January of 2021. Let's say that they -- a company said they were following certain cybersecurity practices during that period --
A. Yes.
Q. -- but they're only following it for a short amount of that period.

Would that be, in your view, a misstatement?
MR. TURNER: Object to form.
THE WITNESS: You know, I don't know that -- I think in that particular set of hypothetical circumstances, you know, I think you'd have to go deeper and, you know -- does it cover 99 percent of the period? Did it cover 2 percent of the period?
Again --
BY MR. CARNEY:
Q. Let's say --
A. -- no --
Q. All right. I'll change my hypothetical then to fit that then.
A. Okay.
Q. Let's say instead of it being from -- the policy being -- follow from October of 2018 to January of 2021, it was followed from October of 2018 to October of 2019, would that be a misleading statement if they said they followed it for that entire period?
MR. TURNER: Object to form without more specifics.
THE WITNESS: Again, we're talking

about, again, in this case, the company saying something -- you know, they -- they performed -- you know, they said they performed a practice and they only performed it for half the time of a period --
BY MR. CARNEY:
Q. Yes.
A. -- I just want to make sure I'm understanding.
You know, in terms of that being false or misleading, I think it would have to link to whether the company -- the company had represented they were following it for the full period or not, right, you know.
Q. Okay.
A. Yeah.
Q. So my hypothetical was they said, we're doing this, let's say it's strong access controls for this entire period, but it turned out they were only doing it for that year.
And I'm just trying to make the hypothetical as simple as possible.
MR. TURNER: Object to form. Object to the term "strong."
THE WITNESS: Yeah, I actually think,

you know, not being a lawyer and not, you know, understanding what, you know, is defined as false or misleading -- right? -- and my job was to just, you know, look at the presence, you know, basically were they doing what they represented. So we might come back to this.

But, like, in determining whether something is false or misleading probably wasn't in the scope for me. It was -- I was trying to determine what -- what they said in the statement, were they doing it, which in all cases of things I examined, they were.

BY MR. CARNEY:

Q. Okay. I'll change my hypothetical to match that then.

Let's say the company said, we have a complex password policy that we followed from October of 2018 to January of 2021.

Do you follow that so far?

A. Yeah. Hypothetical that the company said they had a complex password policy during that period.

Q. Okay.

MR. TURNER: Object to form.

///

BY MR. CARNEY:

Q. And then but in actuality after a year, they just completely stopped enforcing that password policy in 2019.

Would that statement, in your view, not a legal view, be incorrectly describing their cybersecurity practices?

A. I just want to make sure I understand, you know. Is the question whether they, you know, misrepresented on having a policy, or is it a question -- a question of if they stopped -- you used the word "enforcement" in the middle of the period, you know, did they -- I'd have to look at the actual written statement to make a determination of misrepresentation if, you know, they had a policy and then the details around what constituted the drop-off in enforcement to make a determination around this misrepresentation.

Q. All right. Fair enough. I'll adjust the hypothetical to address that.

Let's say after the year, company -- internal email memo said, we are no longer -- have this policy, this complex password policy from now on, but they represented to the public that they had it for the entire 2.5 year period.

A. You know, to the extent to which -- you know, I'd have to understand the context around the email, whether it was an authoritative statement, you know, to the company.

I mean, yeah, so if -- you know, if they -- if they said they were doing something and then, you know -- and in a -- you know, provably factual way they said they stopped doing it during the period but continued to represent that they were -- I mean, in some ways it just goes -- revolves around to if they were saying they were doing it during a period and they, you know, had said that they weren't doing it in the same period, you know, that probably seems to be a misrepresentation.

Q. Okay. Prior to your retention by SolarWinds via Latham & Watkins, had you ever discussed this case with any SolarWinds employee?

A. No.

Q. Aside from your work on this case, have you ever done any other work for SolarWinds?

A. No.

Q. So you've never consulted on cybersecurity issues for SolarWinds apart from this case?

A. That's correct.

Q. Prior to your work on this case, have you ever done any work for Latham & Watkins?

A. No.

Q. And I think it's in your report, but do you recall what your hourly rate is for this case?

A. It's $1,100 an hour.

Q. Okay. And I think you said that you personally billed about 200 hours; is that right?

A. Yeah. Again, I have not looked at each of the invoices over the period. I think that's in the ballpark, but it might be a big ballpark.

Q. And was it -- was it Ms. Lee that you said also worked on the case with you?

A. That's right.

Q. And do you know how many hours she's billed?

A. I don't know how many hours she's billed.

Q. Just quickly, did do you anything to prepare for the deposition today?

A. Yes, I did.

Q. And what did you do?

A. I primarily reviewed my report and Mr. Graff's report, you know, some of the documentation that was cited in both reports, I had discussions with the Latham team.
Q. Okay. Did you meet with the Latham team in preparation for your deposition?
A. Yes, I did.
Q. And how many times did you meet with them?
A. I would say probably three sessions focused on this deposition.
Q. Okay. And were those sessions in person?
A. I was here Monday afternoon and yesterday. So two of those -- you know, two of those were in person.
Q. Okay. Did you speak with anyone else other than counsel in preparation for your deposition?
A. No.
Q. And so how long did you meet with defense counsel in total to prepare for your deposition would you say in terms of hours?
A. Meet with counsel? You know, I would say -- again, focused on the deposition --

right? -- 10, 12 -- between 10 and 15 hours maybe.
Q. All right. Sir, I want to ask you now -- and I'm going to ask you on Exhibit 2, you have an Appendix C at the back. It's the -- I think it's the last appendix --
A. Yep.
Q. -- list of materials you considered in preparing your report.
And did you personally review each of the materials listed in Appendix C?
A. Yes, I did.
Q. And over what time period did you review all of those materials?
A. You know, there's materials, you know, that I received during the course of this. A large amount of the materials, but particularly what I call these tranches of data about the presence of controls, you know, I really only reviewed in October and November of this past fall. So October and November of 2024.
But, again, I had access to some of the documents cited from earlier -- you know, earlier in the proceeding.
Q. Okay. Did counsel choose the documents for you to look at?

A. I --
MR. TURNER: Object to form.
THE WITNESS: Yeah.
MR. TURNER: And object to getting into any conversations with counsel about that.
BY MR. CARNEY:
Q. Yeah. I don't want to get into any conversations. I want to understand what the process by which you received these documents were.
Did you choose them? Did they choose them? How did that come about?
MR. TURNER: Do you want to ask more generally about the types of documents he was interested in reviewing?
BY MR. CARNEY:
Q. I guess I want to understand, did you have a role in selecting what documents you looked at, or did someone else select them for you?
MR. TURNER: Object to the form. "Select."
THE WITNESS: Proceed?
MR. TURNER: Yes, you can.
THE WITNESS: Yes, I did have a role in that.

BY MR. CARNEY:
Q. And what was your role?
A. You know, as I was conducting my, you know, work, I wanted -- I requested to see, you know, documentation, you know, particularly around the implementation of practices and controls.
Q. Okay. Did you provide counsel with search terms to use in looking for documents?
A. You know, to the extent to which I gave language around -- around the types of controls that I was looking for, evidence, you know, of practice, I don't know if we call those search terms or not, but I definitely used language to communicate to them what I was looking for.
Q. Did you have a keyword list that you --
MR. TURNER: I'll object to form.
These are conversations with counsel. I can represent that the witness asked for various types of documents related to the security domains at issue, and SolarWinds tried to provide documents that were responsive to those requests.
BY MR. CARNEY:
Q. And so Solar -- did you have any

communications directly with SolarWinds about the documents that you wanted?
A. I had conversations with SolarWinds, two short conversations with SolarWinds people about questions I had upon looking at the documents. I did not -- I did not request directly from SolarWinds documentation.
Q. Okay. And were those conversations with Mr. Brown and Mr. Kline?
A. That's correct.
Q. Okay. So, first of all, the conversation with Mr. Brown, what did you discuss with him?
A. Again, in both cases, I was just trying to understand some of the more detailed, you know, documentation and how the teams that they were responsible for, you know -- you know, worked with that documentation logging data and those sorts of things.
Q. And were those conversations over the phone?
A. I'm trying to remember if they were Zoom or phone or -- they were remote conversations.
Q. Okay. And were they separate

conversations, your conversation with Mr. Brown and with Mr. Kline?
A. Yes, they were.
Q. And do you recall when those conversations took place?
A. Not specifically. I believe it probably was November '24.
Q. Okay. And was it just you and Mr. Brown on the call, or were counsel on the call as well?
A. Counsel was on the call.
Q. In preparing your opinions set forth in Exhibit 1, did you consider any sources not cited in Exhibit 1 in Appendix C?
A. Can you just sort of restate that?
Q. Sure.
A. I just want to make sure I get the causality.
Q. Yeah. All I'm getting at is, are there documents that aren't sort of reflected or described in your report?
A. No, I don't think so.
Q. Okay. On page 1 of Exhibit 1, paragraph 2, you say, "Having conducted or overseen numerous cybersecurity assessments, I'm

very familiar with how such assessments are ordinarily done.
"An outside expert assessing whether a company has certain controls in place gathers information from people in the company who are knowledgeable about the controls in order to understand how they are designed and looks for artifacts generated from the operation of those controls to ensure that they were implemented."
So I want to ask you about that.
A. Uh-huh.
Q. In this case, you were in 2024 trying to assess whether SolarWinds had certain controls in place during what you described as the relevant period of October of 2018 to January of 2021, right?
A. That's correct.
Q. Prior to this case, have you ever previously been asked to assess whether a company had cyber -- cybersecurity controls in place years earlier than the time at which you were conducting your assessment?
A. Yes.
Q. And when was that?
A. Certainly in the matter that's listed

where I was an expert, the Insulet case. That was the situation there as well.
Q. And what was the situation in the Insulet case?
A. The Insulet case was a trade secret matter, and so it was the plaintiff. And the defendants -- there were questions by the defendants about the presence of reasonable measures that, you know -- in place at Insulet.
And, you know, my -- my role was to assess whether those information security measures were in place.
Q. And were you an expert for the defendant in that case?
A. No. I was an expert for the plaintiff Insulet.
Q. For Insulet.
And you were assessing whether the controls that they said they had in place to protect the trade secrets were actually there?
A. Yeah. I mean, you know, in trade secret cases, you know, the language, I believe, is -- not being a lawyer -- is reasonable measures. So, you know, my -- my expert opinion, you know, talked to the measures they had and

their information security practice.
Q. Okay. And in that case, were you looking at the policies that Insulet had in place, or were you also looking at the artifacts showing the implementation of those policies?
A. Both.
Q. And how many years earlier were you looking from when you were offering your assessment?
A. Many. You know, from -- as -- you know, even earlier to a degree, but probably would call the start date 2007 and -- to about 2014 -- that was the period where, you know -- that was the focus.
Though -- the case did -- did require me to look post-2015, effectively up to the present day. But the focus was in that earlier period.
Q. And did you testify at trial in that case?
A. I did.
Q. And what was the result of that case?
A. Insulet won that case.
Q. Now, sir, in paragraph 3, the first sentence is -- you say, "Applied these standard

practices in assessing whether SolarWinds implemented the practices at issue in the securities statement."
So my question for you is: What are the standard practices in conducting an assessment as to whether a company employed cybersecurity practices years earlier than the time you're looking at?
MR. TURNER: Object to form.
THE WITNESS: You know, in my opinion, you know, having, again, done it in the one case, but in almost all assessments, you're looking to some degree into the past, right? You know, in terms of -- you know, the presence of policies, some of which can be -- have been in place for years.
So I guess is the question about is there a distinction between the methodology for past situations and current situations, or just was is the standard methodology?
Q. Yeah, so why don't we do both.
A. Okay.
Q. Why don't we say what is the standard methodology, and then you can tell me if there's a difference.

A. Okay. Yes. So if -- I'll answer the second question first, there's not really a difference, right, you know?
Q. Okay.
A. So in terms of, you know, how one conducts an assessment, you know, you are looking for, you know, the presence of policy and procedure. You know, evidence that managers, you know, are -- you know, are running those policies and procedures.
Could be through interviews, in the case of SolarWinds, this case, significant testimony through depositions.
And then, you know, artifacts showing those practices and implementation as well as looking at, if it's available, other outside assessments, you know, that are -- you know, sort of who are -- have also been conducted such as we've discussed, the Sarbanes-Oxley and the SOC 2 audits.
So my -- you know, my approach to this practice or what I believe to be standard practice is using those sets of evidence to assess whether the practice is in place.
Q. All right. And I just want to sort of

backtrack to something that I asked you about before the break.
You're not an accountant, right?
A. I'm not. I don't hold a certified public accounting certification, no.
Q. And you don't have expertise as to whether a statement is material within the meaning of GAAP, right?
MR. TURNER: Object to form.
THE WITNESS: Yeah, and I assume GAAP, you're talking about generally accepted accounting principles?
BY MR. CARNEY:
Q. Right.
A. Can you repeat the question?
Q. Sure.
You don't have expertise in whether a statement is material within the meaning of GAAP, right?
A. No.
Q. Okay. And you don't have -- profess to have expertise as to whether an accountant, a CPA would find a statement to be misleading under GAAP, right?
MR. TURNER: Object to form.

THE WITNESS: Yeah, I don't.
BY MR. CARNEY:
Q. Okay. All right. Let me ask you, paragraph 4, which is on page 2, you say -- with regards to Mr. Graff's report, there's a statement down in sort of the middle of the paragraph, you say, "The documents he cites generally have little to do with the practices described in the security statement, et al."
What does that mean?
A. Generally -- right? -- you know, I found that some -- you know, the documents such as some of the emails and PowerPoint documents, you know, were not direct evidence of whether the practices in the securities statement were in place.
Q. But when you say they have little to do with the practices, are you saying they're just completely unrelated to cybersecurity at SolarWinds?
MR. TURNER: Object to form.
THE WITNESS: You know, this sentence, you know, is focused on the fact that those documents are not the most relevant documents related to the practices.

BY MR. CARNEY:
Q. And what do you mean by that? When you say "practices," what do you mean?
A. Things like the presence of access controls or password.
Q. All right. Can you think of an example that he cites as little to do with the practices described in the securities statement?
A. I mean, one would be the -- you know, the FedRAMP assessment.
Q. And why does that have little to do with the practices described in the securities statement?
A. Because that assessment was conducted in a quick and dirty fashion for a budgeting exercise.
Q. But would you agree that the subject of the assessment related to the practices at issue in the security statement?
A. Can you repeat the question?
Q. Sure.
Would you agree that the subject of the FedRAMP assessment related to the practices at issue in the security statement?
MR. TURNER: Object to form.

Are you asking whether the FedRAMP assessment was an assessment of the securities statement?
MR. CARNEY: No. I'm asking -- he said that the documents had little to do with the practices described in the securities statement.
BY MR. CARNEY:
Q. And I'm simply asking whether the FedRAMP items that were being assessed did, in fact, relate to the practices that are described in the securities statement.
A. You know, I just want to make sure, because it wasn't a security assessment and, you know -- you know, it really didn't, you know, have bearing on whether SolarWinds had done the things that they said in the securities assessment, right?
Yeah, I mean, again, that's why I -- you know, that's an example of something that he cites that is really not, in this case, related to the security statement.
Q. All right. Is there an industry standard for determining whether a company has properly employed cybersecurity practices?
A. There are lots of standards about

cybersecurity practices.
Q. But is there a sort of overarching standard that's used in determining whether a company is properly employing the security -- cybersecurity practices it professes to follow?
MR. TURNER: Object to form.
And the witness has already explained what he understood to be the standard approach to assessing that issue.
THE WITNESS: Again, there are, you know, systems and frameworks, you know, promulgated by different organizations around cybersecurity. You know -- you know, my estimation is there's not one overarching singular standard.
BY MR. CARNEY:
Q. Okay. And I guess in a related question, so is there not -- is there a particular standard that you followed in determining whether SolarWinds employed the cybersecurity practices it professed to employ that you're saying that Mr. Graff didn't follow?
A. My assessment was based on, you know, my experience in, you know, the conduct of assessments that utilize a variety of -- you know,

my experience includes assessments that are done under a number of different frameworks, which I've cited in my report.

The assessment wasn't aligned to a specific standard.

Q. All right. Now I want to get into your qualifications briefly.

So maybe if you have -- you have your -- your report, which is Exhibit 1, and then Exhibit 2, we have your CV?

A. Uh-huh.

Q. If you could just open up your CV --

A. Yep.

Q. -- that would be great. So in paragraph 6, it says that you're currently a partner at Next Peak LLC, a cybersecurity consulting company that you cofounded in 2019; is that right?

A. That's right.

Q. And then over on your CV, Exhibit 2, you see it has a similar entry.

Do you see that?

A. Am I looking at two different things or --

Q. Yeah. So I was looking at -- side by

side, I was looking at page 2 --

A. Okay.

Q. -- of Exhibit 1 --

A. Gotcha.

Q. -- sorry about that.

A. No worries. Okay.

Q. And, yeah. So paragraph 6 describes your work at Next Peak; is that right?

A. That's correct.

Q. And then your CV also has a similar entry about that, right?

A. That's correct.

Q. And then in paragraph 6, it says -- the last sentence, it says, "My teams also assist our clients in conducting penetration testing and red team exercises, both of which involve structured testing efforts to find flaws and vulnerabilities in IT defenses."

So have you -- I'm just trying to understand how this works. Have you personally ever conducted penetration testing?

A. I guess my -- can I ask a clarification?

Q. Absolutely.

A. You know, I have had, you know,

oversight of teams. So personally conducted, I have been in rooms during the conduct of penetration tests and red team exercises.

As we've discussed, I'm not a coder, and I did not launch the specific tools during -- you know, during penetration testing and exercises.

I very much read the results, the outputs and, you know, been involved in the determination of, you know, the data we received back and how to report it to the clients.

Q. Okay. And you mentioned that you didn't launch the specific tools. Is that something you could do, though, launch the specific tools for penetration testing?

A. Again, I'm just trying to be precise. I could launch them, right?

I would probably not want myself to be doing that, because you want people that know how to use those tools and have a -- sort of experience and are proficient in them, which is not my expertise.

Q. Okay. And then it also mentions red team exercises.

Have you personally conducted red team

exercises?

MR. TURNER: Object to form.

THE WITNESS: Again, I mean, I think I've answered that in the sense that it -- what I said about being physically present -- you know, designing the exercises, being physically present during their execution. Being part of the team that decided, you know, what we saw in -- you know, and discussed -- you know.

To me that's participation at a deep level in the conduct of the exercise.

BY MR. CARNEY:

Q. Okay. But a similar -- so, first of all, do you need any certain certifications to be able to conduct red team exercises?

A. Legally? I mean, like, required? Required by whom?

Q. Or just from a technical standpoint.

A. Again, required? You used the verb "required."

Q. Right.

A. I'm just trying to -- like, who's requiring it?

Q. Could someone carry out a red team exercise if they didn't have certain technical

certifications?
A. I wouldn't advise that, but it's legally permissible.
Q. Okay. And what type of certifications does someone have who's conducting a red team exercise?
A. There are certifications -- well, again, the conduct involves many people, you know, in terms of design, you know, oversight, you know, technical activity, you know, analysis and reporting.
So, you know, different certifications are probably applicable to different -- to different activities and different qualifications exist across that set of things that, you know, are inherent in the conduct of a red team exercise or a pen test.
Q. Have you taken any formal training in pen tests?
A. Formal training, I have not undertaken any formal training.
Q. All right. Let me move on to the next paragraph. It says, "Additionally, I am the chief strategy and risk officer for Andesite AI, early stage company focused on the improvement of

cybersecurity operations through advanced data science and artificial intelligence."
So -- and looks -- if you look at your CV next to it, it says 2023 to the present.
So you've had both these jobs at Andesite and Next Peak at the same time?
A. That's correct.
Q. And do you collect a salary from Andesite?
A. Yes, I do.
Q. Okay. Are you an owner of Andesite?
A. I have a small amount of equity in Andesite.
Q. And what are --
A. Actually, they're options. So they haven't been exercised yet.
Q. And is Andesite publicly traded?
A. No.
Q. I guess it says right there.
What are your responsibilities at Andesite?
A. I'm on the senior management team. You know, again as -- primarily as the chief strategy officer, I advise the CEO and the board on, you know, the direction of the company,

everything from market opportunity to, you know, the direction of the product.
Q. How do you split your time between Next Peak and Andesite, 50/50 or more at one?
A. It's probably close to 50/50. You know, it very much varies from week to week.
Q. Okay. All right. Okay. If we move on to paragraph 8, it says, "From 2014 to 2019, I was chief information security officer and head of global cyber partnerships at JPMorganChase where I directed its cyber defense program and oversaw more than a thousand personnel in a $500 million budget."
And if be we look over in Exhibit 2 on A-2, second page of your CV, it also says, "chief information security officer and head of global cyber partnerships 2014 to 2019"; is that right?
A. That is right.
Q. So let me break that down.
So from 2014 to 2019, you were what was called the CISO at JPMorganChase?
A. I was the CISO for a year, 2014 to 2015, and then I was asked to take a broader role as the head of global cyber partnerships.
Q. So on your risumi, on your CV, and in

the report, where it says that you were the CISO from 2014 to 2019, that's not accurate, is it?
A. You know, I believe it's accurate to say that I was -- during that period, I was the chief information security and then had a role as the head of global cyber partnerships.
Q. Okay. The second part of the first sentence in paragraph 8 where it says, "Where I directed its cyber defense program," that's the responsibilities of the CISO -- right? -- to direct the cyber defense program?
A. It is the -- you know, the responsibility of the -- the team that CISO is the senior director. I would agree with that.
Q. Okay. And a CISO is the one that directs the cyber defense program, right?
A. Yeah, I mean -- yes.
MR. TURNER: Are you asking at JPMorgan?
MR. CARNEY: At JPMorganChase.
THE WITNESS: Yeah, yeah --
MR. CARNEY: Yes.
THE WITNESS: -- yeah.
BY MR. CARNEY:
Q. So you directed the cyber defense

program at JPMorgan from 2014 to 2015, right?
A. That's right.
Q. You didn't direct the cyber defense program at JPMorgan from 2014 to 2019, did you?
A. From 2015 to 2019?
Q. From 2015 to 2019.
A. That's right.
Q. Okay. So is it fair to say that this sentence here in your report is inaccurate?
A. No. Because the sentence reads I was the chief information security officer and had global cyber partnerships, and I did direct the cyber defense program during that period.
Q. But you only -- you would agree that it says from 2014 to 2019, right?
A. Right.
Q. And you only directed that program from 2014 to 2015; is that right?
A. Right. I think it's, you know, an issue of, you know, semantic interpretation, you know, my interpretation would be that that -- during that period, that was one of my duties.
Q. Okay. And if we look over at your CV on page A-2, it says, "chief information security officer and head of global cyber partnerships,

managing director, JPMorganChase from 2014 to 2019," right?
A. That's correct. The same as the other document. That's correct.
Q. So you would agree that on your CV, it represents that you were the CISO from 2014 to 2019, right?
A. No. It represents that I had two roles, the chief information security officer role and the head of global cyber partnerships role.
Q. So you -- you think that someone reading your report or reading your CV would understand that you were not the CISO from 2014 to 2019?
A. I mean, my CV includes a -- you know, more bullets on things that were head of global cyber partnership roles than they were chief information security officer roles.
So, you know, I think it's -- it's fair to say the reader would understand that some of this was CISO role and some of this was head of global cyber partnership role.
Q. Okay. When -- all right. Let's focus on the second part of that sentence where it talks about more than a thousand personnel.

A. Uh-huh.
Q. When you were the CISO, did you oversee more than a thousand personnel?
A. Yes.
Q. When you were the head of global cyber partnerships, how many personnel did you oversee?
A. A much more limited, again, to my -- you know, number than 1,000. Hesitant to give an exact number, because: A, it changed; and B, I have obligations to JPMorgan not to disclose -- it's a pretty broad obligation not to disclose details.
Q. Would it be fair to say that it was less than 10 people?
A. Not necessarily, you know, yeah. At times it probably was more than 10 people.
Q. Would it be fair to say that it was less than 20 people?
A. Yes.
Q. And when it talks about a $500 million budget, did you oversee a $500 million budget when you were the CISO?
A. Yes. Well -- yes. You know, we were moving to a $500 million budget in the 2015 time frame.

Q. Okay. And, in fact, at the time that you left as CISO, JPMorgan's cybersecurity budget was around $250 million; is that right?
A. I don't -- I don't -- I mean: A, I'm not at liberty to say what it was. You know, and, B, I don't agree that that was the number.
Q. And are you aware of public news reports that JPMorgan planned to increase its cybersecurity budget from $250 million to $500 million over a period of five years?
A. I'm not aware of that public news report.
Q. When you -- when you say that you were asked to go -- I think you described, asked to go into a broader role at the company, is it actually true that you were removed as the CISO in 2015?
A. That's not true.
Q. Okay. Did you -- why is that not true?
A. Because I was asked to take a broader role as the head of global cyber partnerships.
Q. And when you were asked to take the broader role, did you object to being removed as the CISO?
A. I did not. Again, I wasn't removed as

the CISO, so there was no objection to be made.
Q. Well, you were no longer the CISO beginning in 2015, right?
A. That's correct. I was asked to be the head of global cyber partnerships and work with the industry globally on matters of regulation and protection of the financial system.
Q. And within the JPMorgan structure, a CISO is the -- a higher position than the head of global cyber partnerships, right?
A. When I took the head of global cyber partnerships, I was a direct report to the chief administrative officer -- I'm sorry, the -- yeah, the chief administrative officer was actually a higher level of management than the chief information security officer.
Q. Is that Paul Compton --
A. Uh-huh.
Q. -- that was the chief administrative officer?
A. That's correct.
Q. And before you reported to Paul Compton, who were you reporting to?
A. Dana Deasy and Jim Cummings.
Q. And, in fact, Rohan Amin became the

CISO at JPMorgan in 2015, right?
A. That's correct.
Q. In 2014, when you were the CISO at JPMorgan, the company suffered one of the world's largest ever data breaches, right?
A. It actually experienced the breach itself prior to my arrival at JPMorgan.
Q. Okay. And is it fair to describe it that hackers exposed the names, addresses, phone numbers and email addresses of 83 million households and small business accounts?
A. "Exposed" would probably be a mischaracterization.
Q. Is it fair to say that when you -- so you were leading the response to the cybersecurity breach on behalf of JPMorgan; is that right?
A. That's correct.
Q. And is it fair to say that during the time you were leading that response, that you had conflicts with federal law enforcement agencies; is that right?
A. That's not true.
Q. Do you recall having conflicts with the Secret Service?
MR. TURNER: Object to form.

THE WITNESS: No, I -- I mean, I recall discussions with the Secret Service. I wouldn't call them -- I wouldn't call them conflicts.
BY MR. CARNEY:
Q. Okay. Do you know Matthew Zames?
A. I do know Matthew Zames.
Q. Who is Matthew Zames?
A. When I knew Matthew Zames, he was the chief operating officer for JPMorganChase.
Q. Okay. And do you know Joseph Demarest?
A. I do know Joseph Demarest. At the time, I believe he was the head of the -- he was the assistant director of the FBI for cyber.
Q. And are you aware that Joseph Demarest with the FBI called Matthew Zames, the COO of JPMorgan, to discuss delays in access to the breached data that they wanted?
A. I'm not at liberty to talk about the specifics of that incident.
(Whereupon, Exhibit 3 is marked for identification.)
BY MR. CARNEY:
Q. All right. Dr. Rattray, I've handed

you what's been marked as Exhibit 3. And this is a June 30, 2015, article from Bloomberg.
Have you ever seen this article before?
A. Yes, I have.
Q. And when was the first time you saw it?
A. It was published in June 2015. I don't remember distinctly, but I probably saw it not long after its publication.
Q. Okay. So if we can look at the first page of this article, and the article is entitled, "JPMorgan Reassigns Security Team Leader a Year After Data Breach."
In that second paragraph, it says that "Greg Rattray, a former U.S. Air Force commander for information warfare and a cyber expert at the National Security Council under President George W. Bush no longer works as JPMorgan's chief information security officer, according to an internal memo sent June 11 and reviewed by Bloomberg News."
Have you ever seen that memo?
A. I actually don't know what memo this refers to.

Q. Okay. On the next page, it says, "Rohan Amin, a former cybersecurity executive at Lockheed Martin Corp. who joined JPMorgan last August, has replaced Rattray according to the memo."

Was that an accurate statement?

A. Rohan took the job as the chief information security officer.

Q. And then the next sentence says that, "Rattray will oversee a few employees instead of the hundreds he managed in JPMorgan's cybersecurity unit."

Is that accurate?

A. Again, I think the hundreds figure is low. You know, in terms of it numbered over a thousand at that point. You know, I manage a small team initially when I took over and built the global cyber partnerships practice.

Q. All right. And then there's a bold heading that says, "Limited access," and then in the second paragraph, it says, "The Secret Service grew so frustrated that it threatened to seize the evidence, and Joseph Demarest, then assistant director of the FBI's cyber division, called chief operations officer Matthew Zames to discuss -- to

discuss the delays."

Do you have any reason to question the accuracy of that?

A. I do. But I can't go into the specifics of how we handled the incident.

Q. Okay. And then it says, "The situation was resolved with a formal agreement to share information."

Is that accurate?

A. Again, I can't go into the specifics of our interactions between -- or not interactions between JPMorganChase and the federal government.

Q. Okay. So just, sir, turning back to your report, paragraph 8 -- after everything we just discussed and looked at, do you stand by the accuracy of that sentence from 2014 to 2019, "I was chief information security officer and head of global cyber partnerships at JPMorganChase where I directed its cyber defense program and oversaw more than a thousand personnel on a $500 million budget"?

A. Yes, I do.

Q. All right.

MR. CARNEY: Actually, I'm moving on to a different subject. Do you want to take

break?

MR. TURNER: Sure.

THE VIDEOGRAPHER: The time right now is 11:40 a.m.

We are off the record.

(Whereupon, a recess was taken at 11:41 a.m.)

THE VIDEOGRAPHER: The time right now is 11:55 a.m.

We're back on the record.

BY MR. CARNEY:

Q. Okay. Dr. Rattray, I had just a couple quick follow-ups about if we look at Exhibit 2, your CV, page A-1.

A. Uh-huh.

Q. You see where it says, "Cofounder and partner of Next Peak 2019 to the present"?

A. Yes.

Q. And did you hold both those positions from 2019 to the present?

A. Both what positions?

Q. Cofounder and partner?

A. Well, yeah. I mean --

Q. Okay.

A. -- I'm a cofounder and a partner --

Q. Got it --

A. -- yeah.

Q. -- okay.

And then similar with chief strategy and risk officer, Andesite AI, 2023 to the present, did you hold both of those positions from 2023 to the present?

A. Actually, no. I was originally just a chief strategy officer, and then the team decided to do sort of -- formally add "risk officer" to my title.

Q. And when was that added?

A. Spring of 2024, I believe.

Q. All right. And then just with respect to what we talked about on the next page, chief information security officer and head of global cyber partnerships, 2014 to 2019, sir, you'd agree with me that in -- there's nowhere in your report where it mentions that you stopped being the CISO in 2015; is that right?

A. Yeah, it's not relevant to the -- my task, you know, and assessment of the securities statement.

Q. Okay. All right. Let's see. Speaking of security statements, we talked a

little bit about them earlier.
But in terms of the public-facing security statements that we were talking about earlier, what is your understanding of the role that they play?
A. You know, such -- you know, such public statements about security can play a very wide range of roles.
Q. And what are those very wide range of roles?
A. They can be, you know, just awareness that the company, you know, is -- you know, engaged -- you know, engaged in security. It can be, you know, as some of the things that were -- I was involved with, with JPMorgan statements, you know, that support industry efforts in cybersecurity.
They can be -- you know, for the purpose that the SolarWinds statement was for, which is to sort of give people that are thinking about purchasing products some information about security practices of the company.
I mean, the -- it was -- you know, we can continue with this, but there's probably very -- you know, very many purposes for a public

statement about security.
Q. Okay. And based on your experience, for instance, your experience at JPMorgan, do investors care about the cybersecurity practices of the firms in which they invest?
MR. TURNER: Objection to form. And outside the scope of his assignment.
THE WITNESS: Again, I don't -- you know -- you know, I don't know exactly what investors care about, right?
BY MR. CARNEY:
Q. Okay. So when you were at JPMorgan, for instance, was there -- and you mentioned JPMorgan put out public statements about its cybersecurity practices; is that right?
A. At times, you know -- you know, especially related to joining industry associations and those sorts of things, we made statements we were involved with different sorts of security-related activities.
Q. And were -- was one of the reasons that you were making those statements to inform investors about the company's cybersecurity practices?
MR. TURNER: Objection to the form.

And foundation.
THE WITNESS: I don't know, you know -- I mean, how do I -- there were statements made. I'm not aware of statements that were made, you know, specifically to inform investors.
BY MR. CARNEY:
Q. So when you were making these public statements about cybersecurity at JPMorgan, who was the audience for those statements?
MR. TURNER: Objection to form. And foundation.
THE WITNESS: You know, again, in some cases, you know, we -- you know, we were working on, you know, things like the financial services sector cyber risk index that we worked together with NIST on. And there were, you know -- we declared our support for that -- for that effort.
(Whereupon, Exhibit 4 is marked for identification.)
BY MR. CARNEY:
Q. I've handed you, Dr. Rattray, a document that's been marked as Exhibit 4, and it's a publication on Next Peak's website.
A. Uh-huh.
Q. It's called "Building a Focused

Approach to Cyber Defense."
Did you write this article?
A. You know, similar to other discussions we've had, I think the team put it together.
Yeah, so I don't have a recollection specifically about who -- who was the original drafter.
Q. All right. If you would please, sir, turn to the third page of this article.
A. Uh-huh.
Q. Under the second paragraph under the heading "Why Next Peak Can Help," it -- it says, "Many companies, especially in the financial sector, often suffer drops in stock price following a cyberattack, however, JPMC stock actually rose slightly after the breach demonstrating how the steps the companies take during and after an incident can go a long way in reassuring stakeholders."
Do you see that?
A. I do see that.
Q. And do you agree with that statement?
A. I mean, I do agree with those statements. The data we cite is a Harvard Business Review -- Harvard Business Review

article.
Q. Do you agree -- let me break that up then.
Do you agree that the steps that companies take during and after a cybersecurity incident can go a long way in reassuring stakeholders?
A. Yes, I do.
Q. And why was it relevant in your article that the stock price rose at JPMorgan following the attack?
A. You know, the stock -- you know, stockholders are stakeholders in a company, right? And so this is an article meant to sort of portray, you know, concerns and how, again, as you just -- you know, you quoted why Next Peak can help.
Q. And stockholders are investors in the company, right?
A. Stockholders are equity owners in a company.
Q. Okay. And so, in your view, as expressed in this article, stockholders are interested in companies' cybersecurity practices and how they respond to breaches, right?

MR. TURNER: Object to form.
THE WITNESS: You know, the article doesn't say, you know, stockholders are interested. So maybe we need to reframe the question or I need to rehear the question.
BY MR. CARNEY:
Q. Okay. All right.
MR. TURNER: Are you asking him whether stockholders care about public statements like the securities statement, or are you asking about something else?
MR. CARNEY: I'm asking him generally, stockholders care about a company's cybersecurity practices --
BY MR. CARNEY:
Q. -- right? According to your article --
MR. TURNER: I'm just going to object --
(Simultaneous unreportable crosstalk occurs among parties.)
(Stenographer requests one speaker at a time.)
MR. TURNER: I'm going to object. You called two witnesses who you

called to testify about materiality, that issue. Mr. Rattray has not offered any opinion as to materiality. That's not a subject of his report. So I'm just gonna object.
This is outside the scope of his expert testimony.
MR. CARNEY: Okay. And I think under the Federal Rules, you could have just used that last part, outside the scope.
MR. TURNER: Well, I explained why it was outside the scope.
MR. CARNEY: That's called a speaking objection --
MR. TURNER: I understand.
MR. CARNEY: -- which are improper.
MR. TURNER: It's needed in this case. As it may --
MR. CARNEY: There's no provision in the Federal Rules that call for speaking objections being needed, but okay.
THE WITNESS: Are you going to repeat the question?
BY MR. CARNEY:
Q. Yeah. So the question was: The premise of your article that you wrote was that

shareholders could be reassured if a company went out and showed how they were dealing with a cyber breach, right?
A. The premise was -- of the article was that we could help build that focused approach to cyber -- that's the premise of the article.
Q. All right. Sir, I want to ask you about your opinions related to the NIST Cybersecurity Framework.
A. Uh-huh.
Q. And if you look -- I think if you turn to paragraph 31.
A. Of my expert report?
Q. Of your expert report, Exhibit 1, it should be.
A. Uh-huh.
Q. And you say that the NIST Cybersecurity Framework was first established in 2014, right?
A. Again, I made a mistake. I looked at page 31, not paragraph 31.
Q. Yeah, page 10.
A. Yes.
Q. Okay.
A. And I'm on page -- paragraph 31.

Q. Okay. And you state that the NIST Cybersecurity Framework was first established in 2014, right?
A. That's correct.
Q. And that was during the time that you were at JPMorgan, right?
A. Yes, that's correct. Again, I don't know if it was early 2014 and if I had arrived at JPMorgan, but I arrived at JPMorgan in the summer of 2014.
Q. Did JPMorgan follow the NIST Cybersecurity Framework when you were there?
A. JPMorgan -- again, I can't -- I'm going to sort of be limited to how detailed I can go.
JPMorgan led an industrywide effort to, you know, create an industry-driven framework called the cyber risk index based on the NIST Cybersecurity Framework.
What was...
You know -- you know, so, yeah, you know, that was clearly, you know, something that actually I led as the head of global cyber partnerships for the firm and for the industry.
Q. So the cyber risk index was based on

the NIST Cybersecurity Framework?
A. Yes. Or it's actually cyber risk institutes, you know, cyber framework. I'm sorry. I shouldn't have said "index." I should have said "institute."
Q. Okay. And you say it was based on the NIST Cybersecurity Framework.
What does that mean?
A. We were in a situation where the industry was getting from various regulators different -- different regulatory requirements. And as an industry, there was an effort to work to establish a framework that was NIST aligned.
But specific to cybersecurity, NIST had supported such efforts with other industries and supported the effort that we undertook, you know, in the financial services industry.
Q. And did you have any responsibility for ensuring that JPMorgan followed that framework that you just discussed?
A. I was in constant discussions with the leadership team about the nature of the framework that was being derived and how it would enable our, you know, cyber program and compliance.
Q. Okay. When you say "the leadership

team," who was on the leadership team?
A. The CISO, the chief compliance officer of the firm, the implementation people for regulatory compliance within the cybersecurity team.
Q. So who had responsibility at JPMorgan for ensuring that this framework that you just discussed was followed?
A. Again, there was no -- there was -- there was no requirement for compliance with the framework.
Q. Okay. Putting aside a requirement for compliance, was JPMorgan trying to follow the Cyber Risk Institute framework that you discussed?
A. Again, during --
MR. TURNER: Object to form.
THE WITNESS: Right.
Again, that developed over a period of years. JPMorgan, you know, broadly utilized the cyber -- the cybersecurity -- the NIST Cybersecurity Framework, and then, you know, that informed its work on the -- what became the Cyber Risk Institute's framework, which is deeply NIST CSF based.
Just like, you know, NIST called for

as general guidance for, you know, firms to understand their state of practice and, you know, guide -- guide efforts for the NIST Cybersecurity Framework is not something to be followed, per se. It's guidance to enable cybersecurity program.
BY MR. CARNEY:
Q. And so I guess my question then is that JPMorgan -- whatever they were doing with the NIST Cybersecurity Framework, using it as guidance --
A. Uh-huh.
Q. -- who had responsibility for ensuring that they were using the NIST Cybersecurity Framework as guidance?
MR. TURNER: Object to form.
THE WITNESS: Yeah, I mean, the -- there wasn't a singular person. It was a decision, you know, by a number of people, and basically the people that I've described, probably others involved including the general counsel, about, you know, what sort of framework should guide the program in a -- in a heavily regulated environment.
So, you know, there was not a singular individual responsible.

BY MR. CARNEY:
Q. And you -- you said there were a group of individuals.
Were you one of the individuals?
A. Yes --
Q. Okay.
A. -- I mean, okay, yes.
Q. What is the basis for your statement that the NIST Cybersecurity Framework is not something to be followed?
A. You know, I just want to use the quote that I provided in -- in my report, which basically is NIST language around, you know, this is a voluntary -- oh, quoting from the framework.
"The framework is voluntary and there is no right or wrong way to do it."
Q. What page are you on?
A. I'm on page 13, the end of paragraph 36.
Q. Sir, I'm going to ask you -- let me back up for a second.
Did JPMorgan ever perform assessments to see whether it was compliant with the NIST Cybersecurity Framework?
MR. TURNER: Objection to form.

"Compliant."
THE WITNESS: Yeah, I'm not probably at liberty to talk about exactly how JPMorgan self-assessed itself.
BY MR. CARNEY:
Q. Without getting into the details, did they assess themselves under the NIST Cybersecurity Framework?
A. Again, that's a detail, in my estimation. I mean --
(Zoom participant interrupts.)
THE STENOGRAPHER: Excuse me. Can the people on Zoom please mute themselves?
Sorry. If you could repeat your answer.
THE WITNESS: Can we repeat that question?
BY MR. CARNEY:
Q. Sure.
Without getting into details, did JPMorgan assess themselves under the NIST Cybersecurity Framework?
A. Again, I think, you know, the details of JPMorgan's self-assessment probably goes beyond what I, you know, am obligated not to do.

Q. Okay. Putting aside JPMorgan, do you personally have any experience assessing whether a company was compliant with the NIST Cybersecurity Framework?
MR. TURNER: Object to form.
"Compliant."
THE WITNESS: Right. Again, as just described, the framework is voluntary, and there's no right or wrong way to use it. It explicitly doesn't call for compliance. It calls for, you know, voluntarily use in self-evaluation.
To the point of the question, I have numerous experiences helping companies assess themselves under the NIST Cybersecurity Framework.
BY MR. CARNEY:
Q. And what was your role in those assessments?
A. You know, everything from interviewing people about the presence of controls and certain control areas up to working with the leadership team about the -- you know, the outputs of the evaluation and the scoring and even at times in some of the cases helping brief -- brief the assessment company leadership.
Q. Have you ever personally assessed

maturity levels under the NIST Cybersecurity Framework?
A. Yes.
Q. And what was your role in assessing maturity levels?
A. As I just described, everything for certain control areas down to looking at the presence of policy, talking with leaders, looking for specific evidence that control structures were in -- and implementation or active and also looking at other assessments like audit assessments about the presence of the practice.
Q. Okay. Doctor, if you could look at page 62 of your report, please.
A. Page 62, correct?
Q. Yes, sir. And it's paragraph 112, which starts on the prior page.
A. Uh-huh.
Q. And do you see within the body of the report sort of towards the end of page 62, you quote the General Motors Financial Company 10-K for fiscal year 2023?
A. I do see that.
Q. And it states, "We design and assess our program based on the National Institutes of

Standards and Technology Cybersecurity Framework," and then in parentheses, "NIST CSF."

"This does not imply that you meet any technical standards, specifications or requirements, but rather that we use the NIST CSF as a guide to help us identify, assess and manage cybersecurity risks relevant to our business."

Did I read that correctly?

A. Yes.

Q. All right. And you have in footnote in -- in Footnote 145 to that paragraph --

A. Uh-huh.

Q. -- you quote the 10-Ks of Digital Realty Trust and SkyWest; is that right?

A. I just want to make sure that we get the right companies. I see SkyWest. I see GMFC. I'm just -- I'm just looking for the digital real -- there it is. Yep, I see all three companies in the footnote.

Q. Great. And Digital Realty Trust Inc. and SkyWest Inc., they have similar language to the GMFC 10-K statement regarding the NIST framework, right?

A. Yes.

Q. And specifically each of them include

the sentence "This does not imply that we meet any particular technical standards, specifications or requirements but rather that we use the NIST CSF as a guide to help us identify, assess and manage cybersecurity risks relevant to our business," right?

A. Yeah, I would agree that all three companies have similar language in these 10-K declarations.

Q. And what is your understanding of the purpose of that sentence in those three 10-Ks?

A. I couldn't speak to the -- you know, why any given company decided to put that sentence in, because the NIST Cybersecurity Framework lays out itself, you know, in detail that that is the case.

I mean, this says NIST framework is -- you know, does not imply that you should meet any particular technical standard, and it's voluntary to be used as a company sees fit.

Q. Okay. And let's just use the General Motors Financial Company as one example.

A. Uh-huh.

Q. Would you agree that without that sentence, that the meaning of the paragraph is

different?

A. No.

Q. So you think that sentence adds nothing, in your opinion?

A. As I just stated, because NIST basically makes itself -- makes the statements that, you know, are outlined here, we could look at specifics from the framework.

But NIST itself says in publishing the framework that it's not, you know -- does not require or imply that a company does anything specific in terms of technical standards and specifications. And it's meant to be used as a guide.

You know, I find the sentence repetitive and not -- you know, not additive.

Q. Okay. So in the first sentence, it says, "We designed and assess our program based on the National Institutes of Standards and Technologies Cybersecurity Framework, right?

A. Uh-huh. Yes.

Q. And you don't think that that second sentence adds anything to clarify what they mean by that first sentence?

A. I mean, that's up to the people making

this statement about whether they -- you know, they believe -- I believe it's repetitive, because, you know, the NIST Cybersecurity Framework itself tells you the things that are in that sentence.

Q. So one would have to go look at the NIST Cybersecurity Framework itself to understand the first sentence without that second sentence, right?

A. Yeah, I'm just trying to process what the question is.

MR. TURNER: Object to form.

Go ahead.

BY MR. CARNEY:

Q. Yeah, the question is that without that second sentence or some independent understanding of what NIST itself has said about the cybersecurity framework, that first sentence would mean something different, right?

A. No. It would mean exactly what it said, right? Like, we design and assess our program based on the NIST -- the National Institute of Standards in Technology's Cybersecurity Framework. I don't understand how -- I just don't understand how dropping the second

sentence changes the meaning of the first sentence.

Q. Okay. All right. And I'll represent to you that according to the NIST website, the cybersecurity framework is a set of best practices, standards and recommendations.

Do you have any reason to disagree with that?

A. Well, I, yeah, need to see where in the -- you know, the NIST website, which is probably voluminous, because, you know, as stated in my, you know, expert report, it basically says that that -- you know, it's voluntary. And, you know, is to be used as see fit. So it's not directive.

Again, we probably have to compare the language you just said to, you know, other language within the NIST cybersecurity framework's website.

Q. Okay. And you just said the website is voluminous; is that right?

A. Well, you know, as I said, I think it's probably voluminous, because, you know, having been on NIST websites, you know, they -- they sort of link to a lot of things, right?

So I don't know what the front page of the NIST Cybersecurity Framework website looks like at the moment. I don't know what it looked like specifically during the relevant period.

I do know that, you know, it clearly stated, you know, that the framework itself is voluntary and calls on the companies to, you know, use it as they see fit.

Q. And is that -- is somewhere on the voluminous website that it states that it's a voluntary standard?

A. As I said, I don't know for sure if it's voluminous. I said I expect that it is having been on standard-setting organizations' websites many times, and often they are -- they have a lot of links and, therefore, there's a lot of information on it.

I don't know specifically, you know, what instance of the website at what time we're discussing here.

MR. TURNER: I'll note for the record, Mr. Graff is quoting a document that is found on the NIST website as reflected in his report.

MR. CARNEY: All right.

///

(Whereupon, Exhibit 5 is marked for identification.)

BY MR. CARNEY:

Q. All right. Dr. Rattray, I've handed you what's been marked as Exhibit 5. And I'll represent to you that this is a copy of SolarWinds's security statement that the parties have stipulated is basically the way it appeared during the relevant period.

Have you seen this document before or --

A. Yes, I have --

Q. -- some version of it?

A. -- yep.

Q. Sir, if you could turn to -- on the first page where it says -- under organizational security, it says, "SolarWinds follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect and respond to security incidents."

You see that, right?

A. I do.

Q. And you would agree with me that that statement does not have a caveat like the ones that we looked at for General Motors, for Digital

Realty Trust or for SkyWest; is that right?

A. You know, we have the security statement in front of us. It doesn't have a caveat in -- for the -- as I mentioned previously, the caveats were repetitive.

Q. Okay. And if we look at -- on page 62 that we were just looking at in Exhibit 1 underneath the quote from GMFC --

A. Yes.

Q. -- you write, "I understand the representation about the NIST CSF in the securities statement in the same way" --

A. Uh-huh.

Q. -- "not a statement that SolarWinds met any particular technical standards, but rather as a statement about its cybersecurity governance, i.e., a statement that it regularly assessed its cybersecurity posture and used the NIST CSF as a guide in doing so."

Do you see that?

A. I do see that.

Q. So is it -- is it fair to say that even though the securities statement doesn't contain the caveat that the other companies included, you are interpreting it as if it did?

A. I'm just trying to understand the question.

You know, I don't need to -- I guess the -- my thinking is revolving around the notion of the word "interpret," right?

The NIST Cybersecurity Framework itself says it's, you know, not meant to be a set of technical standards, and it's supposed to be a guide to cybersecurity governance.

So there's really, you know, no need for interpretation, because the framework itself calls for this.

Q. Would you expect that, let's say a layperson, someone who is not an expert in cybersecurity, would read SolarWinds's security statement and also read in that limitation or caveat into it?

A. I believe that the security statement is not designed to be read by laypersons. The security statement is meant -- you know, was built and is designed in order to, you know, provide information to potential users of SolarWinds's products about its security practices.

And that to me means the people looking at this have some understanding of

cybersecurity and cybersecurity governance.

MR. TURNER: Chris, just want to flag, the next 15 minutes or so would be good to break for lunch, whenever is good.

MR. CARNEY: Yeah, so why don't we break in 15 then? Is that cool?

MR. TURNER: In 15 minutes?

MR. CARNEY: Yeah.

MR. TURNER: Sure.

BY MR. CARNEY:

Q. All right. I'm going to shift topics now, sir, to ask you about role-based access controls. So if you look at the page 40 of Exhibit 1 -- I'm sorry. Apologies. I just did that myself.

A. Oh.

Q. If you look at page 15, paragraph 40 --

A. Paragraph 40 --

Q. -- and there's a heading that says "The Securities Statement Representations About Role-Based Access Controls Were Accurate."

And I want to direct your attention, sir, to a couple pages forward on page --

A. Excuse me. Just what you -- I just

want to be sure, because I'm reading the first sentence of that paragraph 40, and I don't see the word "accurate" in it. I just want to make sure I'm on the --

(Simultaneous unreportable crosstalk occurs among parties.)

(Stenographer requests one speaker at a time.)

THE WITNESS: Yeah, so I see the heading (c) above paragraph 40 saying the securities statement's representation about role-based were accurate.

Yeah, just to clarify, because I went right to the paragraph 40.

BY MR. CARNEY:

Q. Understand. Thank you.

Sir, if you could turn a couple pages forward, I just wanted to sort of show you what section we were in, but paragraph 44 --

A. Uh-huh.

Q. -- you state, "I have reviewed samples from over a thousand SARFs" -- and that's S-A-R-F, and then plural, SARFs --

A. Uh-huh.

Q. -- "I have received that were filled

out for newly hired employees during the relevant period, evidencing they were completed as a regular practice."

So I want to ask you -- and there's a Footnote --

A. Uh-huh.

Q. -- 28, and by my count, there are eight examples listed there, eight samples.

First of all, who selected these samples for you?

A. As we've discussed, when I asked for evidence of, like, the SARFs, that just some access request forms -- or, you know, evidence of the presence of practice around role-based access control, that I called them data tranches.

The tranche was created for me, and I received it from Latham. I made the selection of the cited examples in the report.

Q. Okay. And how did you go about choosing those eight samples?

A. I reviewed, you know, usually 50 to 70 documents in these tranches and, you know, decided, you know, looked at if the proper number is 8 -- I think -- yeah, I'll just assume it's 8, you know, 8 or 10 in many cases of these large

evidence sets that, you know, sort of illustrative examples from the 50 to 70 that I reviewed.

Q. And putting aside the -- so aside from the 50 to 70 that you reviewed, how do you know what were in the other, let's say, thousand or so SARFs that you didn't look at?

A. You know, similar to, you know, any sort of large data set practice where you're trying to look at -- you know, 50 to 70 is actually a large number to look at in the conduct of an assessment or, you know, of a security control in terms of, you know, getting a sense of whether, you know, this implementation was actually, you know, well -- well conducted in practice.

So I felt like 50 to 70 was more than enough to indicate that the SARF process was in place and executed fully.

Q. Why was 50 to 70 more than enough?

A. Because that's a pretty -- like, there was very little deviation in those samples. They showed the right sort of process, execution. And they're actually very -- sort of very deep in that -- in that sense.

So, again, having done many, many

assessments, that level of sort of evidence examination, you know, is more than sufficient in my estimation to, sort of, you know, validate that -- this element of the role-based access processes was well executed.

Q. Now, to pick the 50 to 70, did you use any kind of sampling methodology?

A. I wanted to make sure I looked across the relevant period, that I looked across different business units, different geographic locations of the company.

Q. Okay. And so what led you, if you did, to believe that the eight samples that you cite in Footnote 28 are representative of the larger body of SARFs at SolarWinds?

A. I chose them based on those same criteria that I just mentioned across that relevant period; business units, to the extent to which I could, and then geographic regions.

Q. The exclusion that you've reached -- I think you mentioned a little while ago that this element of the role-based access processes was well executed.

Was that based on the mere existence of the SARF, or did you reach your conclusions

based on the content of the SARF documents themselves?

MR. TURNER: Objection to form.

And objection -- just --

THE WITNESS: Go ahead. Yep.

MR. TURNER: Yeah, objection to form. And to the characterization of the report.

THE WITNESS: You know, it was basically the second, though, of course -- you know, the fact that they existed was part of the evaluation that their -- you know, a policy and procedure for role-based access was in place.

But, you know, examining that, you know, the reports themselves, you know, my -- my judgment, you know, based upon seeing how this access control is provisioned, you know, and managed in other environments, this seemed a very thorough, sort of above and beyond process for doing so.

BY MR. CARNEY:

Q. All right. So you said basically it was the second.

So you were relying on the content of the SARFs themselves?

MR. TURNER: Objection --

THE WITNESS: No, I said it was --

MR. TURNER: -- vague.

THE WITNESS: Yeah, go ahead.

MR. TURNER: Object to form.

Go ahead.

THE WITNESS: No. I said it was both, right? I mean, I literally said, you know, that the -- you know, the first is important to show that they had a -- you know, general process, you know, for doing this which, you know, I have no reason to doubt was well executed, you know, across the company.

And then I looked at the specific content to make sure that the execution itself was at -- you know, a strong level.

BY MR. CARNEY:

Q. And that's -- when you looked at the specific content, did you only look at the specific content for these eight samples?

A. No. I looked at the specific content for the 50 to 70 samples.

Q. And so what would a SARF document have to include for you to conclude that SolarWinds's access controls were inconsistent with the assertions in the securities statement?

A. I think I want to work a little bit on just what the question is.
Q. Sure.
A. I mean, you know, like, I'm trying to figure out how you could even find evidence in something of inconsistency -- right? -- like, you know, on a given form.
You know, so could you just repeat the question one time?
Q. Sure, sure.
I'm trying to understand, you looked at these SARF documents --
A. Right.
Q. -- and concluded that they were consistent with what SolarWinds said in its public- --
A. Right.
Q. -- facing security statement --
A. Right.
Q. -- right?
A. Yeah.
Q. And I'm wondering what would you have had to have seen in the SARFs, hypothetically, to have reached the opposite conclusion that SolarWinds was not doing what it said in the

security statement?
MR. TURNER: Object to form.
THE WITNESS: You know, again, it would have -- well, first, it would have been a matter of degree of execution, because they had a policy. They, you know, clearly had process -- the SARF process in place.
And it was -- you know, again, lots of data showing its implication. And actually outside auditors had also reviewed the same data and said that this was -- you know, that they were implementing this process and made no findings.
You know, in -- you know, my case, if I had sort of consistently seen that the -- you know, the name field was not filled in, that -- you know, at some large number of the sample -- the 50 to 70 I looked at were missing the name field, that would have been -- that would have been a -- you know, a red flag.
In which case, I probably would have looked to -- you know, talked to the people like I did in those other couple cases we've talked about related to evidence samples about how they used the data.
But, like, I did not see that level of

inconsistency anywhere.
BY MR. CARNEY:
Q. All right. And if you guys can indulge me for a couple more minutes, I have one exhibit related to this, and then we'll break.
(Whereupon, Exhibit 6 is marked for identification.)
BY MR. CARNEY:
Q. All right, Doctor. And take as much time as you need to look at it, but I've handed you what's been marked as Exhibit 6.
And I'm tell you what I did is I took the eight SARFs you cite as samples in Footnote 28, and I put them together as one exhibit. I tried to do it in Bates number order.
But if we can look at the first page, the first SARF --
A. Uh-huh.
Q. -- and it's Bates ending in -- so it's SW-SEC-SDNY- --
A. Uh-huh.
Q. -- 55459, just, for the record.
A. Uh-huh.
Q. You see that an employee named Zouhair Khadija is being requested -- is having access

requested, right?
A. Yes.
MR. TURNER: Object to form.
It's labeled "change in role/access."
THE WITNESS: Oh, okay.
BY MR. CARNEY:
Q. All right.
MR. TURNER: I'm just clarifying that they're not getting access for the first time, if that's what you -- request access.
THE WITNESS: All right.
MR. CARNEY: Thanks for the clarification.
BY MR. CARNEY:
Q. What access was this employee being given?
A. As was just mentioned, this is a change in -- so this, again, is not initial provisioning of access.
This is the portion of the process where SolarWinds also -- you know, if they -- a person changed roles, you know, the process looked through to redefine, you know -- that the role-based access based on the new role.
You know, you see on the reverse of

the form -- right? -- you know, detail about for certain roles, you know, what were the standard accesses for those roles.

So, you know, and then we see system and area under the, you know, "Outlook Distribution Lists." So this -- this entire process, you know, would have re-roled his access in, you know, according to a standardized process that SolarWinds had for different -- different roles within the company.

Q. Okay. And to sort of counsel's objection, clarification, that this was a change in the access that this individual had --

A. Uh-huh.

Q. -- what was it being changed from? What was it before?

MR. TURNER: Objection. Foundation.

THE WITNESS: Again, you know, in this case, it's pretty clear from what's on the form itself that he was going to a new location in Austin and -- you know, a new division, finance. Yeah, so, I mean -- you know.

But, again -- you know, I did not -- you know, analyze every field of every of the 50 to 70 forms nor the eight that are presented.

BY MR. CARNEY:

Q. Can you tell from this form what access rights this employee was given as opposed to what he was supposed to be given?

MR. TURNER: Objection to form.

THE WITNESS: Yeah, you know, this form implements a process that was also described in depositions by the technology leadership that, you know, was meant to, you know, provide a lot of control over what access is.

This is a process that there's a lot of instances on, so they -- they move to, you know, increasing levels of automation even during the period -- you know, the relevant period in the execution of the SARF process.

So I think, you know, in terms of this form in which of the distro- -- like, the -- the role itself has accesses -- you can map to accesses on the back form.

The form would then go to the technology team for implementation. So the form wasn't the only part of the process, right?

BY MR. CARNEY:

Q. Okay. So what would you need to look at to see that the access rights that the employee

was given actually match up with what's on the SARF?

A. What's the question? What...

Q. Yeah, so I'm just trying to understand how we know that this person that accessed this form says they should be given is what they were given. That's all I'm trying to understand.

A. Yeah, I mean, the securities statement calls for the presence of role-based access. There's a process in this form, you know, in -- you know, and the testimony indicates that this form maps directly to accesses that the IT team would implement for different job descriptions like Austin and finance.

You know, the fact that this process is -- you know, robust and detailed, even years after, we can find artifacts about how this was occurred -- makes me highly confident that what they said they were doing, they did.

MR. TURNER: Why don't we break here. You've been going 20 minutes.

MR. CARNEY: Just one more question.

MR. TURNER: One more.

THE WITNESS: Uh-huh.

///

BY MR. CARNEY:

Q. And I'm just asking from, like, a technical standpoint. Zouhair Khadija, if I wanted to know that this person got the accesses that this form indicates they were gonna get back in 2017, what would I look at to make sure it was done correctly?

A. Yeah, I, you know, is this a hypothetical --

Q. No. This is about this person here.

A. Okay. You know, I'm just trying to -- like, the form tells you which of the systems are listed in the back for role -- are you asking whether you're actually gonna go to the person's computer and, like, assess, you know, computer by computer whether that person actually can only get -- you know, has access to the things that are listed in the process, you know -- they can go -- you could go to the person's computer at the point in time and determine whether the accesses -- you know, sort of outlined by the form.

But the point of the securities statement and, you know, the assessment I did was to basically, you know, look at the fact that these things were in place. And this is the

typical way the companies do this.
And the executives of the companies said they did it, and outside auditors also validated that they had proper role-based access control.
Q. Okay. Last question before we break.
What I'm understanding is there's no way you've described an artifact that I can look at now and say -- see that Zouhair Khadija got the specific access controls that are listed in this document; is that fair to say?
MR. TURNER: Objection to form. And foundation.
THE WITNESS: You know, we -- I mean, there could be discovery probably about -- you know, forensic images of his computer. I don't know if those exist or not.
So I'm hesitant to say there's no artifact you could go look for. But it's not necessary in the nature of the assessment I did, because there's deep evidence that there -- you know, that this is an implementation of a practice of role-based access control.
You know, they clearly had process. They were doing the process. The management

testified that that process was in place and being executed. Outside auditors looked at the process and validated that it was in place.
So there was no need to go deeper than this.
BY MR. CARNEY:
Q. All right. Thanks.
THE VIDEOGRAPHER: The time right now is 12:52 p.m.
We are off the record.
(Whereupon, a break for lunch was taken from 12:52 p.m. to 1:49 p.m.)
THE VIDEOGRAPHER: The time right now is 1:49 p.m.
We're back on the record.
BY MR. CARNEY:
Q. Good afternoon, Doctor.
Over the break, did you have any substantive discussions about the case or the deposition with anyone?
A. I did talk to the Latham team.
Q. Okay. About the deposition?
A. Yes.
Q. All right. When we broke, you were looking at Exhibit 6, which was the samples of the

SARFs from Footnote 28 in your report.
A. Yes.
Q. I just want -- one more question about these.
You understand that there are tickets associated with SARFs; is that right?
A. I understand that, you know, SARFs generate user access requests or, you know, tickets.
Q. Okay. And with respect to the eight samples that are in Exhibit 6, did you examine the tickets associated with these SARFs?
A. You know, I -- I examined a number of the tickets. I actually don't remember if I met -- I don't remember mapping those tickets to these SARFs.
Q. Okay. So you're not sure one way or the other whether you looked at the tickets associated with these SARFs?
A. Yeah. That was, again, sort of below the level of analysis that I thought was appropriate -- given that, you know, the fact that both that SARF process and that user access request, you know, tickets really demonstrated what the security statement called for.

Q. What does "below the level of analysis" mean?
A. That, you know, the securities statement, you know, says that SolarWinds has certain processes and practices in place.
And, you know, the approach I took to my assessment, you know -- you know, clearly indicated to me, just as in other instances, you know, that I've done this in the industry and observed others do it, that those were, you know -- that those were in place, things like the process for system access -- you know, implemented by the system access request for forms and the user access request.
Q. Okay. So why don't we just quickly look at what was Exhibit 5, which was the securities statement.
A. Uh-huh.
Q. So on the page ending in 337108, which would be the second-to-last page.
Do you see that?
A. Okay. Yep.
Q. And under "Access Controls," it says, "Role-based access." And so the first sentence says, "Role-based access controls are implemented

for access to information systems."
What is -- what does the SARFs in Exhibit 6 tell you about whether or not role-based access controls were implemented for access to information systems?
A. I mean, this is part of a process of implementation for role-based access controls.
Q. Okay. Is there anything about the SARFs standing alone that tell you that the access controls were actually implemented?
A. You know, there was a -- I mean, the issue is the SARFs don't standalone, right? There's policy, there's the deposition testimony of leaders, you know, that goes into detail about how this access control was implemented.
There are SARFs is one of the mechanisms that are used along with user access requests so -- as well as the fact that outside auditors all looked at the same control set and validated it was in place.
So, you know, the SARFs are not an isolated piece of data related to role-based access control -- or, you know -- yeah.
Q. Okay. And the reason I asked that is because earlier in response to one of my questions

you said that the SARF process and the user access request -- and you said you note tickets really demonstrated what the securities statement called for.
So are you saying that you need to look at more than the SARF and the tickets to see whether this -- what the security statement called for was followed?
A. I think what I'm saying is, you know, the SARFs and user access controls were among the data that I used, you know, to -- example, you know, the presence or practice around role-based access.
As I've said many times, I used -- you know, common, you know, approach in the industry of, you know, looking for policy and procedure, you know, talking to or looking at depositions of management about how they implemented these things, artifacts like the SARFs and the UARs.
And, you know, the fact that in many cases, outside audits also look at the same controls. So, you know, that -- it was the approach that I took across all of the areas that I evaluated.
Q. Okay. And, Doctor, let me just ask

you one more question about that -- one more sentence in that paragraph. The third sentence says, "Access controls to sensitive data in our database's systems and environments are set on a need-to-know/least privilege necessary basis."
Is there anything about the SARFs that we're looking at in Exhibit 6 that show you that statement that I just read you about the need to know least privileged necessary base was followed?
A. Well, again, the SARFs are, again, part of a system of implementation about need to know and privilege.
You know, they -- they do provision. You know -- they're part of the process of provisioning a user with a proper, you know, access at the least privilege necessary level.
Q. So you would agree then that SARFs and the tickets alone don't demonstrate that the securities statement was followed with respect to access controls, right?
MR. TURNER: Object to form. Mischaracterization of testimony.
THE WITNESS: As I said, the SARFs and the user access -- yeah, the user access request can't -- can't be taken in isolation in evaluating

a part -- you know, an aspect of the security statement.
And there's a much richer set of evidence about the presence of these controls that I did use.
BY MR. CARNEY:
Q. Okay. So can you, maybe just to clarify for me, why it wasn't necessary to look at the specific tickets associated with these SARFs you used as examples?
A. You know, as is typical, when, you know, people are assessing something like the practices, you know, there's a rich set of evidence which, you know, I can, again, repeat in terms of the presence of policy, clear deposition statements about how that was executed by management, strong documentation, you know, SARFs, user access.
Again, auditors also looking at these process and saying there was sufficient evidence to say that these things were in place, you can't go down to the -- you know, the specific level on any specific form and, you know, and look at it.
It's just beyond the scope of what was necessary to see that the securities statement

depicted, you know, SolarWinds's conduct in a way that the readers of the securities statement would expect.

Q. All right. Sir, if I could ask you to turn to page 20, paragraph 45.

A. Of -- yeah, my statement. I see.

Q. Yeah. Sorry. Of Exhibit 1.

A. Uh-huh.

Q. And you see there's a paragraph there, paragraph 45 that talks about tickets. And if you turn over to the next page, you say, "As with the SARF forms, I have reviewed samples from thousands of these tickets I received from the relevant period evidencing that they were generated as a regular process as part of the SARF process."

Do you see that?

A. Yeah. I just want to orient a bit.

Are we talking about the bottom of page 21?

Q. So what I just read was from the top of 21, and then it has a Footnote 36 at the bottom that has the samples, I believe, of the tickets that you selected; is that right?

A. I mean, what I'm reading is, "As with the SARF form, I reviewed samples."

Is that what you were quoting?

Q. Yes.

A. For me, that's on the bottom of page 21, just to be -- just to be precise about it.

Q. Are you looking at Exhibit 1?

A. Oh, you know what? I'm probably looking at Exhibit 2. Sorry.

And the page reference?

Q. Page 21, please.

A. 21.

Q. 20 over to 21.

A. Okay. Yeah, I just want to make sure I read the context for it properly.

Q. Sure. Of course.

(Pause for reading/reviewing.)

A. Okay.

Q. Similar to what I asked you earlier, how were the samples that you have in Footnote 36 selected?

A. In a similar fashion as with the SARFs.

Q. And I'll represent that I counted that you have nine samples listed in Footnote 36.

A. Uh-huh.

(Whereupon, Exhibit 7 is marked for identification.)

BY MR. CARNEY:

Q. All right. As with the SARFs from Footnote 28, I put together the tickets from Footnote 36 --

A. Uh-huh.

Q. -- as one exhibit. And I'm not going to go through all of them, but if we look at the first page, the first ticket, do you know what employee this relates to?

A. You know, in terms of, you know, which employee, I don't know specifically. I assume, you know, that it's Makins Rickey. But, you know, I did not analyze each of these forms in detail.

I mean, I analyzed the nature of the form, but I didn't look at the specific, you know, data in each field of the form.

Q. Okay. And if we look at that first page ending in 49602, down in the notes, if we look at the bottom note, does it appear to relate to someone named Mark Fraser?

A. Can you point me a little more generally to what I'm looking for?

Q. Sure. Sure. If we look at the ticket

info in the subject line, it also mentions Mark Fraser.

Do you see that?

A. Again, I -- which -- I may be looking at the wrong --

Q. On the first -- the first page.

MR. TURNER: It's right here.

THE WITNESS: Oh.

BY MR. CARNEY:

Q. 4960.

A. Okay. Yeah, well, I see an email down at the bottom, two lines, the very bottom with an email from Mark Fraser.

What else am I looking at here?

Q. I'm just wondering if that sort of refreshes your recollection or helps you understand that this ticket relates to Mark Fraser rather than Rickey Makins?

A. That was, again, below the level that I was looking at these, you know, tickets in this case.

You know, the presence of the tickets sort of clearly indicated that the things that management said were in place, were in place in terms of a process for role-based access and, you

know, implementing that.
You know, I did not -- did not feel it was necessary to look at the implementation in each specific example.
Q. And just to be clear, I'm just talking about the nine examples --
A. Uh-huh.
Q. -- that you cited in your report.
You didn't think it was necessary to look at those?
A. I mean, I did look at them, and I selected them.
Q. Okay. Can you tell what access level this employee was being given?
A. I -- the person who would have received this would have been the person that needed to be able to, you know, interpret what each of these fields are.
I'm very confident that, you know, this process, you know, allowed, you know, the recipient of a user access, you know, request to, you know, conduct the process properly.
You know, as you can see, the forms are complicated and -- you know, I wasn't trained as a SolarWinds, you know, recipient of this

ticket, so I don't know exactly.
Q. Did you look at the SARF associated with this particular ticket?
A. No. I didn't feel like I needed to. But I was looking for in both cases, the SARF process and these tickets, was the existence of the process which clearly demonstrated SolarWinds had a role-based access approach that, you know, was utilized in order to, you know, appropriately provision access.
Q. How does the existence of the process tell you that it was appropriately used?
A. Well, you know, again, I didn't rely solely on the artifacts that showed existence of the process.
There was testimony by the management under oath and depositions that the process was being conducted. There were other outside assessments that also found the same.
So, you know, as we've been talking about quite a bit, the assessment I did, it wasn't necessary to get to the level of, you know, mapping each individual, you know, ticket to its execution, because I don't think that's necessary.
I mean, we're sort of making the

assumption that they would do all this for -- you know, and not actually conduct all the activity. These processes are heavy weight and, you know, in place in order to accomplish what was in the security statement.
And it's pretty clear that, you know, the reader of the security statement would understand that, you know, SolarWinds was doing, you know -- meeting the representations in the security statement.
Q. In your mind, is having a process in place mean that the process is followed?
A. Is this a hypothetical question?
Q. Not really. It's just I'm wondering if you see that --
A. I mean, just in general outside of this specific situation?
Q. Yes.
A. And, again, could you create a process document and do nothing to implement it? That's possible. But it's clearly not the case in what we see here with SolarWinds.
Even these documents, which are not process documents, they're implementation documents demonstrate, you know, efforts to

implement the process.
Q. And you said could you create a process document and do nothing to implement it.
How about could you create a process document and not implement it correctly? Is that possible?
A. Again, we're sort of abstracting out of any specific in the SolarWinds case?
Q. Yes.
A. Yes. Improper process implementation is theoretically possible.
Q. And in the case of -- let's use the SolarWinds SARF ticket process.
What would you have had to have seen to know whether or not the process was being implemented improperly?
A. You know, again, my assignment was to sort of evaluate the security statement and, you know, assess whether the things that were, you know, asserted there were in place.
You know, clearly, you know, the presence of, you know, not just process documentation but many, many artifacts of implementation indicated that the process was there.

It wasn't my role to look at sort of at the granular level, you know, the implement -- the exact implementation of it in detail. I mean -- you know, at an instance-by-instance detail.

Q. So is it fair to say that at a high level, in this case, you're offering the opinion that during the relevant period, as you've defined it, the SolarWinds security statement was not inaccurate or misleading?

A. It is my opinion that the SolarWinds security statement was -- was accurate.

Q. Okay. And it's your opinion that by virtue of that, this securities statement was not misleading?

A. Yeah, I do not believe the security -- the SolarWinds security statement was misleading, no.

Q. Is it fair to say that's sort of the crux of your expert opinion?

A. You know, the crux of my expert opinion was, you know, as detailed in my expert report. I looked at the security statement, you know, focused on particular areas that I -- you know, believe are at issue in the case.

And, you know, saw evidence of a variety -- you know, variety of sorts that indicated the assertions made in the security statement were true.

Q. All right. Sir, if I could ask you to turn to page 23, paragraph 49.

A. Uh-huh.

MR. TURNER: Can you just give me a minute, Chris. I'm having trouble tracking down Exhibit 1.

MR. CARNEY: Oh, I might have another copy, if you want.

THE WITNESS: Did I steal that one too? I don't think so.

(Whereupon, discussion held off the written record to find document.)

THE WITNESS: Exhibit 1 again.

BY MR. CARNEY:

Q. Yes, sir. So page 23, paragraph 49.

A. Okay. You know, may I have a quick moment to just read the paragraph?

Q. Of course. Anytime you need that, just --

A. Okay.

(Pause for reading/reviewing.)

A. Okay.

Q. Okay. Sir, in the last sentence of paragraph 49 you say, "Again, I have samples from numerous SARFs I received requesting such changes along with corresponding tickets evidencing that this practice was commonly followed during the relevant period."

So I want to ask you about that.

What does it mean that it was commonly followed?

A. Again, with the SARF that I received with tickets, it looks like they were executing the practice, which was the level at which I was trying to, you know, see that direct evidence of the practice and implementation.

That, you know, I was not looking to statistically analyze the full -- the full set, you know. So commonly followed was -- with the evidence I saw, it was followed.

Q. When you say you were "not looking to statistically analyze the full set," what do you mean by that?

A. Well, I think it sort of -- I didn't look at every SARF related to a change, and all of the corresponding tickets and -- and do a

statistical analysis, because it was unnecessary as we've assessed quite a bit.

You know, the process -- you know, the clear, deep, you know, documents -- you know, documentary evidence that they had these processes and they were doing them is the level at which my analysis was conducted and is -- you know, the level of analysis that I think would be expected in terms of the security statement.

Q. Okay. And you'd agree, commonly followed doesn't mean uniformly followed, right?

A. If you're asking that, you know -- is the question that -- I'm just trying to understand --

Q. Sure, sure.

A. -- you know, is the question that -- whether, you know, I'm asserting by saying "commonly followed" that every -- every SARF or, you know, for change was done perfectly?

Because, yeah, it definitely doesn't mean that they achieved the standard of perfection.

Q. Okay. And just picking up on your comment about not having done a statistical analysis, so it's fair to say you didn't look to

see what percentage of the time this process was followed, right?
MR. TURNER: Object to form.
THE WITNESS: You know, we've discussed this a lot, and I've -- we may do it quite a bit this afternoon. That was out -- you know, outside the scope on the sense that, you know, I had multiple sources of information that, you know, clearly indicated -- you know, that SolarWinds was doing the practices, in this case, proper role-based access control that the securities statement; and, therefore, you know, I did not do an analysis of, you know, every instance of the SARFs across the entire relevant period.
BY MR. CARNEY:
Q. Okay. And let me just ask you a hypothetical then --
A. Uh-huh.
Q. -- this is not SolarWinds, just a hypothetical.
If the access -- companies' user access policy was followed 95 percent of the time, but the 5 percent of the time that it was not followed involved elevated permissions being

granted to employees who should not have had them, would your opinion change about whether the -- following it -- what's the word? I'm sorry, let me -- whether following it commonly was enough?
MR. TURNER: Object to form.
THE WITNESS: Again, you know, the statement we've been reading this last sentence of paragraph 49 is not the sole basis for my, you know -- you know, my assessment that SolarWinds's security statement related to role-based access is correct.
There's many, many other sources of information that sort of indicated that they were doing the things that there are in the security statement.
You know, in terms of a statistical -- you know, the 95/5, I mean, it's very hypothetical. I would have to understand a lot of context around the company of concern, you know, again -- you know, the -- the errors in why that error rate.
But that was out of scope for, you know, the exercise here, which was to look at the securities statement and, you know, assess whether SolarWinds was, you know, performing as they

affirmed they were performing in the security statement.
BY MR. CARNEY:
Q. Okay. All right.
(Whereupon, Exhibit 8 is marked for identification.)
BY MR. CARNEY:
Q. All right. Doctor, you've been handed what's been marked as Exhibit 8. And I'll represent to you that these are the -- in that last sentence of paragraph 49 we just looked at, you say that you, "have samples from numerous SARFs I received requesting such changes along with the corresponding tickets."
And that -- so these appear to be the samples that are in Footnote 44 --
A. Okay.
Q. -- do you see that?
A. Yes.
Q. And so first of all, would you -- if you could just flip through this --
A. Uh-huh.
Q. -- are all these documents tickets or any of them SARFs, as you understand, in your Footnote 44?

MR. TURNER: I'm just confused. The footnote is citing what I assume are SARFs, and then it says, "I understand the tickets have been produced with the corresponding SARFs attached."
Maybe I read it backwards, but...
MR. CARNEY: Right. So I'm just --
MR. TURNER: The footnote is referencing both, and there's obviously attachments missing here.
MR. CARNEY: You say there's attachments missing.
MR. TURNER: It says -- the footnote says, "I understand the tickets have been produced with the corresponding SARF forms attached."
So if these are the tickets, I assume there were SARF forms attached to the production, and they're missing here.
MR. CARNEY: Okay.
BY MR. CARNEY:
Q. All right. And you can -- you can look through -- you can look through the Bates numbers that are cited in Footnote 44 and tell me if I'm missing any of the documents that you cite to in that footnote.
MR. TURNER: We can go off the record

if you like. I think, Maurice maybe can explain this.

But I think basically if you -- the way the documents were electronically produced, the SARFs were an attachment to the document just like with an email.

MR. BAYNARD: I believe the tickets were produced earlier and then we produced the SARF form [indiscernible].

THE STENOGRAPHER: I can't hear you.

MR. BAYNARD: That we produced the SARF forms later with an overlay so they were linked in the review database so you could see the attached ticket -- further attached form to each ticket.

MR. CARNEY: Okay.

BY MR. CARNEY:

Q. And with that --

MR. TURNER: So there was no way -- I just -- to clarify, so I'm not sure there's a way of citing to SARFs directly.

MR. CARNEY: So you're saying they don't have Bates numbers, is what --

THE WITNESS: That may be.

MR. BAYNARD: They have Bates numbers,

but they just aren't sequential, because they were produced at a later date.

MR. CARNEY: Okay. And thank you for that clarification.

BY MR. CARNEY:

Q. So, Doctor, would you have looked at the SARFs that are associated with the tickets that are listed in Footnote 44?

A. Yes. As we were just discussing, you know, as these -- as this evidence was produced, you know, I looked at it.

I don't know that I can map each one of these to the SARF, but, you know, there is a -- you know, again, I think we just heard, there's a process for that.

But, you know, again, I clearly looked at these tickets, you know, to the notion of this paragraph, which is there was an implementation, you know, in place for the change process.

I think if you read through these, it's pretty clear that they were implementing -- you know -- they were implementing changes to -- you know, role-based changes.

Q. Okay. And I was really just trying to understand from a technical standpoint if you

followed the process that Mr. Baynard described and looked at the associated SARFs?

MR. TURNER: If -- just to make the record clear, I think that what happened is the documents were produced to Mr. Rattray before they were produced to y'all in the form we just discussed.

So he may have gotten the tickets with the SARFs attached, but in order to produce them to you, the tickets had already been produced, so we were overlaying them with those so they wouldn't appear as attachments. It's complicated.

MR. CARNEY: Okay.

MR. TURNER: But as far as I understand, Mr. Rattray would have received them originally as tickets, and attached --

(Simultaneous unreportable crosstalk occurs among parties.)

THE WITNESS: And I would have reviewed that as a group, if they were -- if the SARFs were attached to the tickets.

BY MR. CARNEY:

Q. Okay. And do you recall whether the SARFs were attached to the tickets when you looked at these samples?

A. You know, I believe they were. But, again, as you can -- you know, you can well see, there was a lot of evidence we were working through.

Again, my assignment was to make sure that the tickets in this case from SARFs related to changes, that the process -- you know, the SARFs generated tickets and the tickets were acted upon.

Q. Okay. All right. And once again, I don't want to go through all these tickets, so let's just use one as an example. If we look at the first page --

A. Uh-huh.

Q. -- ending in 47323, can you tell what type of access request change is being made here?

MR. TURNER: Just take your time --

THE WITNESS: Yeah --

MR. TURNER: -- to read through the document.

THE WITNESS: -- uh-huh.

Again, as we look at what, you know, this filled out ticket, you know -- where, again, I was looking at not any specific access change but the presence of a process and, you know, an

implementation of a process for ticketing to make sure the changes got done.

You know, I read a sentence that please note that Andy is not [indiscernible].

THE STENOGRAPHER: I can't understand you.

THE WITNESS: Okay. Yeah. So as I read this, there's a sentence that says, "Please note that Andy is now an employee of SolarWinds MSP UK. Can his access be amended to reflect the change from contractor to employee?"

So I believe, you know, that would probably be the -- you know, the access change requested.

BY MR. CARNEY:

Q. And what's the difference in access from a contractor to an employee at SolarWinds?

MR. TURNER: Objection. Foundation.

THE WITNESS: You know, I don't know the specifics of what systems contractors get versus employees.

As we've talked about a lot, it's clear that SolarWinds had a process to control and properly provision role-based access, and that's what I was looking for.

BY MR. CARNEY:

Q. All right. Sir, if I could -- you can put that one aside.

A. Uh-huh.

Q. If I could ask you to turn to page 24. You state -- and you can -- if you need -- at any time, if you need to read back to get context --

A. Uh-huh.

Q. -- please feel free, but it says, "All these are the source of artifacts I would look for had I been hired in the ordinary business context to conduct an assessment of SolarWinds's role-based access controls.

"In my opinion, they easily demonstrate that the representations in the securities statement relating to role-based access controls were true."

And then you --

A. I'm just trying to -- I'm actually not tracking where you are reading.

Q. Oh, sorry. I'm on page 24.

A. Exhibit 1.

Q. Exhibit 1. Paragraph 52.

A. Okay. Got it. I'm now seeing it. Yeah. I may read this contextually when you

finish --

Q. Okay.

A. -- but why don't you please proceed.

Q. Sure.

So I just read that -- that paragraph to you. I won't read --

A. Yeah. You don't need to read it again --

Q. -- it again?

A. -- but the first two sentences of paragraph 52.

Q. Got it.

And then you quote from the security statement regarding access controls.

Let me just focus you on the last sentence --

A. Uh-huh.

Q. -- it says, "Access controls to sensitive data in our database systems and environments are set on a need-to-know/least privilege necessary basis."

How -- you state in paragraph 52 that the artifacts you looked at easily demonstrate that the representations in the securities statement relating to role-based access controls

were true.

And can you just explain to me how these samples that we just looked at easily demonstrate to you that SolarWinds was only allowing access on a need-to-know/least privilege necessary basis?

MR. TURNER: Object to form. Mischaracterization.

Go ahead.

THE WITNESS: Okay. The whole SARF process where, you know, role-based access is basically the same as need-to-know, right?

So, you know, we've had the discussion about these SARFs and tickets that I've reviewed, you know, being -- you know, among the evidence I used for role-based access, and, again, which is synonymous with need-to-know.

So, you know, that's why I made -- that's why I'm confident in this statement.

BY MR. CARNEY:

Q. And just to make sure I'm understanding, the individual SARFs and tickets that you looked at by themselves don't demonstrate to you that the representations in the securities statement relating to role-based access controls

were true, right?
MR. TURNER: Object to form.
THE WITNESS: I've answered, I believe, this -- pretty much the same question, right?
That the SARFs -- and, you know, the associated tickets were an element of a -- you know, an element of a system and a set of, you know -- a subset of their total amount of data that I used to, you know, make the assertion that all of these are the sorts of artifacts I would look for, right?
So I looked for these for presence of implementation in the form of, you know, a process, which the SARF -- the SARFs show how they did. System access request and the tickets show how that was -- you know, how that moved through to the implementation.
So, you know....
So that is how I made -- you know, made the judgment in this case.
BY MR. CARNEY:
Q. Can you have role-based access that is not synonymous with a need-to-know basis?
A. Are we talking about some sort of

hypothetical situation?
Q. Yes.
A. Yeah, probably want to avoid any kind of given hypothetical. But role-based access is the way companies, you know, as common practice and language now, you know, handle access controlling.
And, you know, in the case of the securities statement, you know, that's the expectation of the reader of the securities statement and, you know, vendor management teams is to see that a company like SolarWinds, when you're buying their products, you know, understands that they need to have role-based access in place.
I mean, that's what the purpose of this statement is, and that is why I examined what I examined.
Q. All right. Sir, if I could direct your attention to paragraph 53, which is on page 25 of Exhibit 1.
A. Okay. Sorry. I went to -- before all I should say, remember, Greg, it's paragraph 53 not page 53. I'm there, paragraph 53.
Q. Okay. And then it goes over on to the

next page.
A. Yep.
Q. And in that paragraph, you discuss user access reviews.
Do you see that?
A. I'm going to read the paragraph --
Q. Sure.
A. -- so -- yeah, just so we can proceed when I have enough context.
(Pause for reading/reviewing.)
(Whereupon, Exhibit 9 is marked for identification.)
THE WITNESS: Yeah, I've read paragraph 53.
BY MR. CARNEY:
Q. And in Footnote 51, you cite a number of samples of user access reviews that you looked at, right?
A. Yes.
Q. Okay. I -- all right. And I'll just tell you this Exhibit 9, I think this was printed out in the native format, so it doesn't have the Bates number on it, but this would be the first sample in Footnote 51, which is SW-SEC-00296522.
A. Yes.

Q. And have you looked at this particular user access review before?
A. You know, the user access reviews cited in Footnote 51, I looked through each of those.
I mean, basically clicked through, you know, extensive set of, you know, user access reviews, right? Do I remember, you know, that this one is Bates numbered -- each particular Bates number here, I do not.
Q. I would not expect that, sir.
But the format of this, does this look familiar --
A. Yes.
Q. -- to user access reviews you looked at?
Okay. Can you tell from looking at this user access review who conducted it?
A. Let me just take a quick look through the whole thing.
You know, in terms of who conducted it, you know, I think one perspective on the question is "who" might not be the right word.
Because user access reviews are probably generated as a -- I mean, in many places

are generated as a normal set of data production out of an automated system in order to make sure that you're reviewing who had access, right?

So, you know, especially the -- you know, the deep long, you know, fields and fields of data that we see are clearly, you know, outputs from, you know, an automated logging system.

So I'm not sure there's a single who associated with the generation of this.

But what I was looking for was, you know -- and, again, you know, as the -- as the paragraph says, you know, as we'd talked about SARFs and user access forms, the fact of regular user access -- you know, regular review of user access rights is just an additional layer of confirmation for the processes, you know, outlined in the securities statement.

Q. Okay. So rather than who conducted it, what system was used to generate this user access review?

A. You know, I asked for production of, you know, data related to -- you know, role-based access control, and user access reviews were highlighted as one of the sources of information that showed the implementation of the processes.

So in terms of the exact way these were generated, I did not and felt like it was not necessary to understand that. Having seen many types of document -- process documentation, this looks very clean and organized.

And to the extent to which, you know, do I feel this provides good granularity and ongoing confidence that SolarWinds reviewed the access their users had, this data set, you know, to me very clearly indicates that that was the case.

Q. And what makes this data set clean?

A. Just well organized, right? You know, in terms of, you know, the fields that are in here, the account types that are in here.

You know, again, cleaning and pretty comprehensive, right? You know, the locations, the names, the email addresses, right?

You know, in terms of, you know, output that would, you know, show that a process existed in addition to the, you know, SARF and, you know, user access ticketing process that they're actually reviewing it and confirming that their role-based access program was in place, this is good documentation of that.

Q. And what, if any, conclusions can you draw about whether user access was only allowed on a need-to-know/least privilege necessary basis from looking at user access reports like this?

A. You know, again, the assertion that I made in the -- regarding the security statement in terms of need-to-know and least privileged was the presence of the system that, you know, the role-based access system of which this is just one cross-check on that system.

And so, you know, these user access reviews allowed -- you know, would allow for checking whether the process of, you know, provisioning of users was -- you know, the data there to check that it was done properly.

Q. Okay. All right. Sir, if I could ask you to please turn to page 65 of your report.

In paragraph 119, it starts at the bottom. And you can look at paragraph 118 might be help -- provide some context too.

A. Uh-huh.

Q. You're talking about a help desk ticket that Mr. Graff cited.

Do you recall that?

A. Yeah. If it's okay, I just would like

to read 18, 19 --

Q. Sure.

A. -- and maybe 20 just so I get the full context?

Q. Of course.

(Pause for reading/reviewing.)

A. Okay. I think I'm ready.

Q. All right. So if you look -- now that you have the context, if you look in paragraph 119, the second sentence, you say, "First, it's not even clear from the chat that the one-year time period was incorrect. The person who specified the time period may have gotten it from the temps manager."

I want to stop right there.

Have you seen any documents indicating that the person who specified the time period got it from the temps manager?

A. Well, first, shouldn't we be looking at the artifact we're talking about here?

Q. If you would like to, sure.

A. Yeah, I mean, that would be useful.

(Whereupon, Exhibit 10 is marked for identification.)

MR. CARNEY: And just for the record,

I've handed you Exhibit 10. And that is the artifact that you requested, and it's Bates number SW-SEC-SDNY_00050922.

THE WITNESS: Okay. Yeah, I got the artifact.

BY MR. CARNEY:

Q. Okay. So my question was: In paragraph 119 of your report, you say, "The person who specified the time period may have gotten it from the temps manager."

And I asked: Have you seen any evidence to that effect?

A. You know, I think, you know, in the -- the general context here, that the point being made in that sentence is there are a lot of explanations for what might or might not be on this form.

But that this is one form out of thousands of, you know, SARFs. And the specifics here, which, again, I've said, you know, I was trying to illuminate that, you know, we don't know exactly how any specific form, you know, would be filled out.

In terms of the question, have I seen, you know, evidence that the -- you know, that

the -- that the person who needed the time period defined could have gotten it from the temps manager, I have not seen such evidence.

But as we've talked a lot about, I didn't go to that level of analysis. I was sort of asserting here or saying here, there's a lot of reasons that this form could have been filled out the way it is.

Q. Okay. So when you make the statement, "The person who specified the time period may have gotten it from the temps manager," you were speculating; is that fair?

A. Oh, yeah. You know, it was sort of with a distant illustration of, you know, more fundamentally by focusing on this particular, you know, ticket.

You know, the fact that a SARF has, you know, ambiguity at this level is not the level I was operating on for this assessment.

It's that they had a SARF process, right? If you look -- if you look at the SARF and the dialogue, it shows that they're trying hard to figure out what is appropriate access, right?

Like, they're not just willy-nilly implementing things. There's a dialogue with

notes. That is, you know, strong implementation of a -- you know, a role-based access and control system.

Q. All right. So instead of focusing on the one ticket, in the second part of that sentence in paragraph 119, you say, "Or that period may have been a standard employment period for a temp."

Do you see that?

A. I do.

Q. Okay. Have you seen any documents among the thousands of SARF tickets you had access to indicating that the one-year period was a standard employment period for a temp?

A. This is a -- I think another example of I wasn't looking for documentation at that level. This was just illustrative of why there might -- you know, what might be going on, you know, in the case of this SARF.

And, again, to illuminate the fact that they had a very strong process. And that, you know, there wasn't a need at my -- you know, for me to see if they had a role-based access control process, like, stated in the securities statement to look for that level of sort of

procedure -- you know, procedural execution.

Q. Okay. So is it fair to say that when you said the period may have been a standard employment period for a temp, that you were speculating?

MR. TURNER: Object to form.

He's already explained the purpose of the remark.

THE WITNESS: Yes. And as you know, I can repeat the entire statement I just made. Hopefully the record will -- you know, will show that that wasn't my task to determine, you know, all the specific procedural implementation.

This paragraph was meant to say, in any specific case, you know, there may be good reasons for why this SARF is the way it is. But more fundamentally, they had a SARF process.

This SARF indicates a strong effort to make sure that it was implemented in a thoughtful way. And that was sufficient for me to affirm what was in the securities statement.

BY MR. CARNEY:

Q. Okay. In that same paragraph towards the end, you mentioned that, "A separate SARF would be submitted upon an employee's

termination."
Do you see that?
A. I do.
Q. Have you seen the SARF ticket decommissioning this temp's access after they left the company?
MR. TURNER: Objection. Assumes facts not in evidence.
THE WITNESS: You know, I think we're -- we're gonna have the same conversation once again. You know, the point of paragraph 119 is that -- to show that there's a lot of reason any individual SARF may have been written the way it is.
But my -- you know, my expert report, you know, starts the next paragraph with, "But more fundamentally."
And this is the point; that one particular SARF is really not -- not relevant to judging whether SARFs or more generally the full set of evidence, you know, presented around the presence of role-based access is sufficient for me to determine that, you know, I feel confident that the securities statement is -- is accurate.
///

BY MR. CARNEY:
Q. All right. Sir, I'm going to switch topics to -- I'm going to ask you some questions --
THE WITNESS: Can I ask for a break? I have to go to the bathroom.
MR. CARNEY: Sure, sure.
THE WITNESS: How long have we been going?
MR. TURNER: An hour.
THE VIDEOGRAPHER: The time right now is 2:52 p.m.
We're going off the record.
(Whereupon, a recess was taken at 2:52 p.m.)
THE VIDEOGRAPHER: The time right now is 3:04 p.m.
We're back on the record.
BY MR. CARNEY:
Q. Dr. Rattray, if I could ask you to please look at page 35 of Exhibit 1, paragraph 67.
A. Okay.
Q. You say, "There's clear evidence in the record that SolarWinds did enforce password complexity on active directory."

And then, "In particular, I have reviewed a chat between Tim Brown and Eric Quitugua," and then you go on to describe the chat.
Do you see that?
A. I do. I'm just going to -- as we've been doing the last little while, I just want to make sure I've got the context for things as, you know, we go into your questions.
MR. TURNER: Go ahead. Take the time you need for it.
(Pause for reading/reviewing.)
THE WITNESS: Okay. I think I'm good for a moment.
BY MR. CARNEY:
Q. And so you see paragraph 67, the chat you reference?
A. Yes.
Q. And Mr. Quitugua sends back a screenshot in the chat; is that right?
A. Yes. I -- yeah.
Q. Is that correct?
A. Yes, it -- that's right. You know, it happened in 2017, which was quite a bit outside the relevant period, but, yeah, I see that.

Q. And so if it happened quite a bit outside the relevant period, why did you rely on that chat?
A. Because I think it, you know, was just the start of the process which would have continued into the relevant period.
Q. Okay. So you would agree that in assessing the cybersecurity practices of a company, it is acceptable to review and rely on chat messages between employees regarding those practices, right?
MR. TURNER: Objection to form.
I think he's relying on what's depicted in the chat message.
MR. CARNEY: Okay. Speaking objection, that's completely improper.
MR. TURNER: I'm just clarifying the objection. It was objection to mischaracterization of testimony.
MR. CARNEY: How did I mischaracterizes it? He relied on the chat.
MR. TURNER: He's relying on the screenshot that's in the chat.
MR. CARNEY: Which is part of the chat, so your speaking objection --

MR. TURNER: You're speaking now. I'm trying to just clarify. If you left it there, I wouldn't have to keep speaking.
MR. CARNEY: Okay. You're coaching the witness during a deposition.
MR. TURNER: Go ahead, Chris.
MR. CARNEY: It's improper. I don't like it. It's against the Federal Rules of Civil Procedure.
MR. TURNER: Chris, I made a very short description about the form that I was objecting to.
Please continue.
MR. CARNEY: All right.
BY MR. CARNEY:
Q. Doctor, so would you agree that in assessing the cybersecurity practices of a company, it is acceptable to review and rely on chats messages between employees regarding those practices?
A. You know, the set of evidence I relied upon, you know, in this case, you know, looked at a chat that showed, you know, direct evidence of the -- you know, password -- you know, how active directory, you know, was -- was utilized, right?

So, you know, the evidence is that, you know, active directory in the following paragraph discussing how Microsoft guidance around password complexity. You know, in my case, that's the evidence I was relying upon.
Q. Okay. And as you indicated, it was from quite a bit outside the relevant period, right?
A. Right. The point there being they put this in place early as they were -- you know, as testified in multiple places, you know, increasingly using active directory so that active directory, you know, was increasingly the -- the source of implementation of password complexity.
Q. Okay. And you would then also agree that in assessing the cybersecurity practices of a company, it is permissible to look at documents from outside the relevant period you're studying, right?
A. In the case of showing that things were in place earlier that had every -- you know, reason to believe were continued and in this case testimony that says active directory was the primary place at which SolarWinds was seeking to -- you know, manage identity.

You know, in this case, it was useful to show that that had been in place, because it was -- there's a whole evidentiary basis to say they were increasing the use of active directory.
Q. If I can ask you, sir, to look at page 87, paragraph 158.
A. Page 87.
Q. Yes. Thank you. In the last sort of clause of that paragraph, you state that there's evidence establishing that, "SolarWinds generally implemented password controls in a manner consistent with the representations in the security statement."
Do you see that?
A. Again, I'm going to read all of 158, and then -- yeah, I'll answer the -- I'll ask you to repeat the question, and I'll answer.
Q. Okay.
(Pause for reading/reviewing.)
A. Okay.
Q. And my question was about the statement that "SolarWinds generally implemented password controls in a manner consistent with the representations in the security statement."
Do you see that?

A. I do.
Q. And what did you mean by the word "generally" in that sentence?
A. You know, as we've been discussing throughout the day, you know, my task was to look at the security statement and, you know, examine whether the things in the security statement were, you know -- there was -- you know, the presence of process and procedure and implementation.
And I saw that consistent with the representations in the security statement.
Q. All right. If I could ask you to look at -- hopefully you still have in front of you Exhibit 5, the securities statement.
A. [Speaking sotto voce]. Got it.
Q. On the second-to-last page with the actual text on it, the page ending in 337108.
A. Yes.
Q. And under "Access Controls" and then under "Authentication/Authorization," do you see the sentence that says, "Our password best practices enforce the use of complex passwords that include both alpha and numeric characters which are deployed to protect against unauthorized use of the password."

Do you see that?
A. Yes, I do.
Q. And you'd agree that this assertion does not include the word "generally," right?
A. The word "generally" is not in the sentence you just read.
Q. And do you agree that the statement would be different if it included the word "generally" in it?
MR. TURNER: Objection to form.
THE WITNESS: Different -- different how?
BY MR. CARNEY:
Q. Would it have a different meaning if that same sentence I just read had the word "generally" in it?
MR. TURNER: Object to form.
THE WITNESS: I'm not sure in the context of the securities statement that's even true. I don't necessarily agree with that assertion.
BY MR. CARNEY:
Q. Why is that not true?
A. Because the securities statement is, you know, a document that is, you know, depicting

to, you know, the vendor management people who read it is the narrow -- you know, the purpose for this securities statement.
And, you know, all -- all it's meant to do is, you know, illuminate that SolarWinds understood the types of controls that they had and that they were -- there were practices in place.
So, you know, whether you said generally we do that, because no one's holding this to a bar of perfection, or we are -- our parts were practices -- you know, in terms of the use of this statement, I'm not sure it does make any difference.
Q. If I could turn you back now to paragraph 65 of Exhibit 1. I'll give you a page number.
A. Okay.
Q. Page 33.
A. Uh-huh.
Q. You state that --
A. Oh --
Q. I'm sorry. Paragraph 65 --
A. -- I did it again.
Q. -- paragraph 33.
A. Yeah, I'm there.

Q. All right. And you can -- I'm going to ask my question. You can have as much time as you want to read for context.
But you say, "Given this context, my understanding of the securities statement's representation that SolarWinds's best practices were to enforce the use of complex passwords is that SolarWinds's automatically enforced password complexity through technical measures where it was feasible to do so."
Do you see that?
A. I do. I'm going to take a moment just to make sure I read the, you know, entire paragraph so that I understand, you know, the full -- the full context.
(Pause for reading/reviewing.)
A. Okay.
Q. Okay. Regarding that first sentence that I just read in paragraph 65 where it ends with, "Where it was feasible to do so," do you agree that the securities statement does not include the phrase "where it is feasible to do so"?
A. That --
Q. With respect to passwords?

A. Right. I'm just trying to -- I'm just reorienting myself to that sentence.
The sentence, you know, doesn't need to, you know, say "as feasible to do so," you know, in the sense that you can't do things that aren't feasible. It doesn't -- so, therefore, the wording's unnecessary, but it's not there.
Q. So what would it mean for it to be not feasible to do so?
A. You know, in terms of, you know, enforcement of password complexity, you know, it needs to be done through technical measures, you know, in order to -- to, you know, automatically enforce as, you know, that sentence you read said, you know.
Therefore, you know, because you would need the technology in place to automatically enforce, which is the best -- which is the best practice being referenced here, again, that's -- you know, that's why the language about not -- you know, the language is missing related to feasibility, because it's unnecessary.
Q. Okay. And if I could ask you to look at the securities statement again --
A. Uh-huh.

Q. -- you should have it in front of you, that same page we were looking at.
A. Right.
Q. And in that same paragraph under "Authentication/Authorization," it states, "Our password policy covers all applicable information systems, applications and databases."
Do you see that?
A. I do.
Q. And what does that mean to you?
A. That means there are written, you know, guidance to the -- the company, you know, is applicable to all -- applicable -- you know, all applicable to information systems, applications and databases.
Q. And, once again, you would agree it doesn't say "where feasible to do so," right?
MR. TURNER: Objection to form.
THE WITNESS: Yeah. Correct. That sentence doesn't have the clause that says, "where feasible to do so."
BY MR. CARNEY:
Q. And is it fair to say that you're reading that into the securities statement?
MR. TURNER: Objection to form.

Objection to the characterization of the report and the testimony.
THE WITNESS: Okay. That's -- repeat the question again, please.
BY MR. CARNEY:
Q. When you state in paragraph 65 that you understand the security statement's representation that SolarWinds's best practices were to enforce the use of complex passwords, that that means that SolarWinds automatically enforced password complexity through technical measures where it was feasible to do so, you're reading the phrase "feasible to do so" into that paragraph of the securities statement, right?
MR. TURNER: Objection to form to that sentence.
THE WITNESS: You know, as, you know, the paragraph goes on to state, you know, their user access process narrative, you know, talks about the fact that, you know, the use of active directory as a, you know, automated means of password complexity through technical measures, it was the focus here.
And I think the securities statement is just noting for a potential, you know, vendor

management team that there was -- you know, where feasible, the -- you know, again, you don't need to -- didn't need to say it. I added it to the -- to paragraph 65.
But, you know, that for enforcement, you need automation, and that -- you know, that was how they enforced password best practices where it was feasible.
BY MR. CARNEY:
Q. Okay. And just to address my friend Mr. Turner's objection.
Does the "where it's feasible" concept apply to the sentence that says, "Our password policy covers all applicable information systems, applications and databases"?
A. No. Because the two sentences are pretty distinct, and they're -- you know, what they're trying to articulate. That, you know, they're -- the overall password policy, you know, is -- is a general obligation, you know, across those applicable information systems, applications and databases.
The best practices language, you know, necessarily is about enforcement. And you can enforce where it's feasible to do so.

So the -- as written in paragraph 65, the feasible -- you know, the "where feasible to do so" language applies to the best practices were used to enforce complex passwords.
Q. And you mentioned just a little while ago vendor management, and I think -- you can correct me if I'm wrong, but the securities statement was addressed towards vendor management; is that right?
A. Yeah, that's my understanding.
Q. And what does "vendor management" mean to you?
A. To me, you know, vendor management teams are teams that are assessing, you know, a supplier.
In this case, SolarWinds is a supplier of products. And, you know, among many things they do, one of the things they do is look at, you know, those organizations.
And, you know, do they have the proper security in place, is the risk -- you know, what sort of risk does that product pose?
So my understanding is that origins of this security statement were meant to provide, you know, those type of teams an understanding of what

SolarWinds's practices were.
Q. So in your use of the word "vendor," SolarWinds would be the vendor?
A. Right.
Q. Okay.
A. The team -- just to be -- just as a clarification, the vendor management teams would be talking about would be diligencing or looking at SolarWinds and potentially the securities statement, because, yeah, SolarWinds was selling something, and the vendor management team was looking at SolarWinds.
Q. All right. Sir, I'm going to ask you to turn to -- let me give you a page number -- page 45 --
A. Uh-huh.
Q. -- paragraph 83.
A. Yep.
Q. And it's -- it's in the section where you're talking about software development --
A. Uh-huh --
Q. -- do you see that?
A. -- yep.
Q. And you touched on a little bit your involvement in overseeing the software development

lifecycle at JPMorgan.
Do you recall that?
A. Yeah, it was one of the places where I was involved with that security aspects of software development, yes.
Q. And did JPMorgan follow a waterfall or an Agile process?
A. You know, during -- during the period I was there, there were actually -- you know, it was a large organization, and at -- they were moving towards an Agile process in some software development.
I would imagine, you know, that some of it was still developed by a waterfall, very contextually -- you know, contextual.
Q. Okay. So if we flip forward a few pages to paragraph 90 on page 49, you state in the middle of that paragraph, "I have reviewed various guidance documents from Confluence" -- and that's with a capital C --
A. Uh-huh.
Q. -- "that indicate SolarWinds followed an Agile development process."
And you say, "In particular, I've reviewed a document titled 'Security Testing

Process' created in 2016 and last updated on June 22, 2018, focused on how security testing was integrated into the process."
Do you see that?
A. I do. Once more, I just think it's easier for us, can I review that paragraph 90 --
Q. Sure.
A. -- and just make sure I got -- I got the full context -- for this.
(Pause for reading/reviewing.)
A. Okay. Let's proceed.
Q. Okay. So in the sentences that I read, first of all, there's a Footnote 106 and you refer to a document as a -- and you can read Footnote 106, but as a "slide deck from 2015 explaining basics of Agile process, including the bug 'scrub' done during each sprint."
Do you see that?
A. Uh-huh.
Q. And here we can...
(Whereupon, Exhibit 11 is marked for identification.)
BY MR. CARNEY:
Q. And just for the record, I've handed you what's been marked as Exhibit 11. And this is

the presentation you reference in Footnote 106 and begins with Bates number SW-SEC-SDNY_00184276.
A. That's right. And if you don't mind, I'd like to just take a moment and --
Q. Sure.
A. -- look through the full presentation as we go forward.
(Pause for reading/reviewing.)
A. Okay.
Q. So, sir, just my question: Why did you rely on a slide deck from 2015 for your understanding as to SDL practices SolarWinds was following in what you defined as the relevant period of October 2018 to January of 2021?
A. You know, similar to the other discussion we had, you know -- I -- you know, if you look at the full set of evidence, including, you know, Mr. Colquitt's deposition, he -- he was building on this foundation, right?
So, you know, using this foundation where they were, you know -- you know, this deck is pretty foundational in terms of, you know, how to do Agile. This was a foundation that they -- they built upon.
So this was -- you know, the document

really, you know, got to the point that: A, they were using Agile, and, B, the security testing process was part of how they did Agile. You know, it was the best illustration of that.

Q. And if we turn to the third page of this document --

A. Uh-huh.

Q. -- ending in 276, do you see there's a -- there's an agenda on there?

A. Are we talking about the contents page?

Q. Yeah, the contents page.

A. Right.

Q. Exactly.

A. Yeah.

Q. With time allotments --

A. Uh-huh.

Q. -- including for a break?

A. Right.

Q. Is it your understanding that this was part of a presentation?

A. You know, I don't -- it does appear to be part of a presentation -- or not part of a presentation. It looks like a deck that is meant to be presented --

Q. Okay.

A. -- you know, which is maybe a different answer.

Q. And do you know who it was presented to?

A. You know, this is, you know, pretty clearly a deck that is meant to be presented to technologists related to the development process.

Q. And so would you agree that in some instances, it's appropriate to review slide decks to gain an understanding of the cybersecurity practices that a company is following?

MR. TURNER: Objection to form.

THE WITNESS: You know, there -- you know, this slide deck, you know, was used to evidence that SolarWinds had, you know, moved to the Agile process and that security was present.

It was, you know, it was part of the full set of evidence along with Mr. Colquitt's depositions and other technology leaders about how they implemented the Agile process and the security processes associated with it.

You know, it's an element of the evidence I examined.

///

BY MR. CARNEY:

Q. Okay. In paragraph 94 on page 52, you -- I'll let you get to that.

A. Okay. Yes. I'm going to read the paragraph about the final security reviews.

(Pause for reading/reviewing.)

A. Okay. Yeah.

Q. Okay. In that paragraph 94, you describe final security reviews or FSRs as "the most significant artifacts I've reviewed from SolarWinds's software development process."

So let me ask you: Why are these the most significant artifacts?

A. Well, you know, again -- or this is in the context of the more general discussion of, you know, the software development lifecycle and the security aspects of it.

So, you know, the most significant, you know, related to the fact that, you know, these were -- these final security reviews demonstrated, you know, both, you know, deep process related to, you know, how they approached, you know, secure development.

As -- you know, as well as, you know, lots of -- lots of the supporting evidence for

other elements of the -- you know, the implementation of evidence in addition to the other sources of evidence that exist for the implementation of things like testing processes.

Q. Okay. In paragraph 95, you talked about -- that you reviewed a sample from approximately 100 FSRs you received.

Do you see that?

A. That's right.

Q. And who selected the samples that you looked at?

A. You know, it was similar to the other -- I call these evidence tranches. I may have said that before. I think we were talking about the SARFs, but maybe others as well.

I requested, you know, evidence from the Latham team of, you know, implementation -- you know, implementation including things like, you know, the outputs of implementation processes like final security reviews.

So they selected -- they selected the hundred.

Q. And then you selected the -- I'm going to -- I think I counted 14-or-so samples that are identified in Footnote 120?

A. Right. Similar process. I looked -- in this case, I know I looked at more than 50, but, again, that 50 to 70 in this case as well.

And then I selected the subset that I've cited in the report.

(Whereupon, Exhibit 12 is marked for identification.)

BY MR. CARNEY:

Q. Okay. Dr. Rattray, I've handed you what's been marked as Exhibit 12. And, for the record, this is just the first sample that you identify in Footnote 120 of the FSR, and it starts with the Bates stamp SW-SEC-SDNY_00055119.

And could you just help me, just walk me through this FSR, tell me what it shows.

A. I'm gonna just read it through myself real quick --

Q. Sure.

A. -- and then, you know, I'll walk you through it.

Q. Thank you.

(Pause for reading/reviewing.)

A. I looked through it.

How should we proceed? Do you want to ask the question again and, you know, give me some

parameters for the walkthrough?

Q. Yeah. How about I'll just ask you, to speed things up.

Can you just tell me how documents like this FSR establish to you that, if it does establish that to you, that SolarWinds followed all aspects of the SDL in its securities statement?

A. Again, the FSRs were an element of the determinations I made around, you know, SolarWinds's, you know, software development and, you know, the statements made in the securities statement.

You know, the presence of this review as process and the type of, you know, implementation that we see in these reviews, you know, is a pretty strong, you know -- you know, not pretty.

It's a very strong, you know, capstone on a -- on a set of the processes outlined in the securities statement.

You know, it includes things like requirements analysis, back to our -- you know, its phase, there's a template, there's a series of things with structure that guide the -- the

development process from a security perspective, you know, so that the teams that are, you know, working on a given product or application, you know, are guided -- you know, guided in this fashion.

So, again, it has requirements analysis. Again, as we talked about things like threat -- threat modeling, you know, understanding security requirements are part of the element of things like threat modeling.

It talks to the type of testing outlined in the security statement. It even requires scheduling of testing early. Shows test -- testing results of a variety of sorts, you know, all the phases outlined in the security statement, you know, mapped here including to the sort of product security review.

You know, this is the -- this is a -- a process that constitutes product security review, you know, shows -- shows that the appropriate players were involved in the -- you know, the review -- an approval phase, phase 4.

Q. So you mentioned that it shows testing results of a variety of sorts.

Is it -- does this Exhibit 12 do that?

Does it show test results?

A. I see checkmarks reports specifically as test results.

Q. What page are you on?

A. I'm on the second page.

MR. TURNER: For the record, it's on all four pages.

THE WITNESS: Oh, yeah. Fair enough. Second page, third page --

MR. TURNER: From the first as well.

THE WITNESS: -- and the last page. Yeah, yeah, bottom of the first page.

BY MR. CARNEY:

Q. And there are -- so are you saying that there are test results in this document, or that it links to other documents that purport to contain test results?

A. No. There's test results in this document. The checkmark report and the data there, you know, high, medium, low, you know, as stated in basically all pages are test results.

Q. So just for the record, the results themselves are in this document?

MR. TURNER: Just object to form.

Go ahead.

THE WITNESS: Yeah, it's a question of what you consider results. But, you know, the -- the results summary in terms of high, medium and low are -- you know, the test results are summarized here, you know, in a few places as checkmark report and I believe -- yeah, dates are given.

And it looks like there's a link to the PDF where the more detail, you know, report would be available.

BY MR. CARNEY:

Q. And did you look at that more detailed report?

A. I looked at a large number of testing reports including checkmarks report.

Q. Did you look at the testing reports associated with the samples that you have in Footnote 120?

A. No. Similar to the other sets of data, I was looking for the existence of the right process and clear evidence of its implementation.

You know, in the case of the security reviews, I've been looking at testing reports, again, just to, you know, know or confirm that, you know -- that the checkmark -- you know, the

types of things that were in their checkmark reports, how those reports were organized, there was absolutely no reason for me to believe if they listed a checkmark report in any FSR, it wouldn't -- you know, it wouldn't be there.

It would be a lot of work, you know, to create summaries of results from reports that didn't exist. I felt no need to look at the specific reports when it was very clear that the testing was, you know, going on.

Q. Okay. And in that same paragraph, the last sentence, you said that, "The FSRs included sections for engineers to post links to tickets," and in parentheses, you have, "(stories) in JIRA concerning security issues found and addressed through security testing, as well as places to post summaries of or links to results with vulnerability scans and penetration tests."

Can you show me where in this Exhibit 12 are the sections for the engineers to post links to tickets concerning security issues found?

MR. TURNER: I have to object here.

Because this issue is noted in Footnote 120. I want to make sure you've seen

that.

The problem is these can't be printed today with the links live, but the linked documents were produced separately and covered in the footnote.

BY MR. CARNEY:

Q. Okay. And to counsel's whatever that was, did you look at the linked documents?

A. There was a set of linked documents produced, and I did look at those.

Q. And did you look at the linked documents for the samples that you selected in Footnote 120?

A. The -- you know, the -- you know, looked at a produced set of links. Again, you know, in the process of producing, you know, the material, you know, both for the security review and the presence of supporting, you know, JIRA -- JIRA-based documentation, as -- it was just described, you know, that turned out to be not at the same time.

So I didn't have the FSRs with the -- I'm sorry, had the JIRA tickets associated with an FSR in sort of a single production.

You know, I made an effort to -- you

know, when I went through the JIRA reports to, you know, look at, you know, as process, the types of things they linked back to.

I did not map every, you know -- every FSR to the JIRA reports that I was looking at, because as we've been discussing today, that sort of analysis was well below the level necessary to sort of understand that the securities statements, you know -- you know, illumination.

Or when the security statement said there was a secure development process -- you know, set of activities, you know, such as testing activities, the final security reviews provided, you know, strong evidence of that, you know, that I saw that were linked to issue identification.

I saw tickets that indicated that that -- you know, that -- those JIRA links did exist, right? They were broken in some of the FSR documentation.

And that this robust process was, you know, being executed and, you know, met -- you know, met what I needed in terms of how the industry would approach validating that the things in the security statement, you know, such as pen testing and static testing were in place.

Q. Sir, if I could ask you to turn to paragraph 101 of Exhibit 1.
A. Uh-huh.
Q. And this is on page 56.
And you're discussing what you perceived to be problems with Mr. Graff's methodology, right?
A. Yeah, I should, again --
Q. Okay.
A. -- read these as you start to ask questions. Is that -- I shouldn't assume that's fine.
Q. Of course. Of course.
(Pause for reading/reviewing.)
A. Okay.
Q. In paragraph 101, maybe it's the fourth sentence down, you say, "Cybersecurity assessments generally do not involve reviewing employees' emails or presentations to management in the first place."
And then parenthesis, "(let alone stray comments or notations in such documents that lack appropriate context)."
Do you see that?
A. Right.

Q. We looked at -- a little while ago, you relied on a presentation that documented what you thought was the company's SDL process, right?
MR. TURNER: Object to form.
THE WITNESS: If we're talking about the presentation about Agile -- right? -- you know, it included, you know -- it included how Agile is conducted and then security steps during Agile development.
BY MR. CARNEY:
Q. Okay. And you made an assessment using your cybersecurity experience that it was appropriate to rely on that presentation from 2015 to -- in forming your opinions, right?
A. That was an element of, you know, what I looked at. You know, I looked at, you know, unlike Mr. Graff, you know, the policies, a very large set of documentary evidence, you know, process, things like FSRs.
I used that document because it was a good baseline, as we said, about what they were -- you know, how they understood that process of Agile and where a security fit into it, but it was not the base -- you know, the sole basis of my, you know, assessment of their secure development

practices.
Q. But you exercised your judgment and determined that it was appropriate to look at that particular presentation, right?
A. Yes.
Q. Okay. And with the chat we looked at earlier with the screenshot, you exercised your judgment and determined that it was appropriate to look at that particular chat with the screenshot, right?
MR. TURNER: Object to form.
THE WITNESS: Right. You know, the sentence, you know, continues to say, "let alone stray comments or notations in documents."
You know, in the case of the PowerPoint presentation on Agile, it was a full presentation that was, again, illuminating that -- this sort of foundational, you know, movement and conceptualization of SolarWinds in that area.
It was not a single notation inside, you know -- you know, inside a presentation. It was, you know -- it was a -- sort of the full presentation. You know, I felt like it was -- it was very useful in illustrating how -- you know, how they were thinking about this, which was what

I was trying to do there.
You know, as we discussed in the case of the email, it was, you know, documenting Microsoft's, you know, process. It was contained within an email, but the point was active directory, you know, had strong -- the ability to implement strong -- strong passwords.
So it wasn't an opinion. It wasn't a comment. It was, you know, linkage to a global technologies company's, you know, product and its features regarding strong passwords.
BY MR. CARNEY:
Q. Okay. Let me ask you, please, to turn to paragraph 121. And this is on page 67.
A. Uh-huh.
Q. And I'll just let you know that paragraphs 121 through 126, you discuss this issue of developer access to billing data for test purposes.
And you can look -- as we go along, you can look --
A. Uh-huh.
Q. -- at as much of it as you want to get context. But I'm gonna hand you the email that's -- that you're discussing.

A. Okay.
(Whereupon, Exhibit 13 is marked for identification.)
THE WITNESS: I'm going to take a quick moment and, you know, just read the material and the statement related to this situation.
BY MR. CARNEY:
Q. Okay.
(Pause for reading/reviewing.)
A. I just want to familiarize, you know...
Yep. I'm ready.
Q. Great.
So you've been handed what's been marked as Exhibit 13 --
A. Uh-huh.
Q. -- and this is an email chain that you reference in Footnote 160 of your report, and it's Bates stamped SW-SEC-00254254.
A. Understood.
Q. All right. So if we could -- I just want to see if we can agree on some things.
If we go to the second-to-last page of this document --
A. Uh-huh.

Q. -- which is -- ends in 265.
A. Okay.
Q. And if we look at that email -- because these threads are obviously in reverse chronological order.
A. Yep.
Q. If we look at that email at the bottom from Sean O'Shea, it says in the first bullet, "They're currently using a shared login currently of a different SolarWinds employee. This is definitely a security incident and needs to stop."
Do you agree with that sentiment, that this was definitely a security incident that needed to stop?
MR. TURNER: Objection to form. Foundation.
THE WITNESS: You know, the -- the identification of this is an incident and, you know -- and I'm also aware that they did, you know -- yeah, they -- they treated this, you know, with a lot of, you know, attention.
So I guess -- if the question is: Is -- you know, is the fact that a different SolarWinds employee using a password as a security incident, yes.

BY MR. CARNEY:
Q. Great. And that's --
A. Okay.
Q. -- all I was asking. Thank you.
And based on your cybersecurity experience, why is that a security incident?
MR. TURNER: Object to form.
THE STENOGRAPHER: Excuse me. I couldn't hear you.
MR. TURNER: And the term "incident."
THE WITNESS: The sharing of -- this is a -- you know, are we talking about this specific situation or just generally password sharing?
BY MR. CARNEY:
Q. Well, you had said in your prior response that a fact that a different SolarWinds employee using a password is a security incident, and I'm just trying to understand why it was a security incident.
A. You know, again, just sort of generally password sharing, you know, is not seen as something that should occur, and, you know, security policies, you know, user -- you know, user access policies where people are told about

what -- how they should use their -- use their access, you know, you generally don't -- you know, generally say you should not do that.
Q. Okay. And would sharing login information violate any of the tenets of the SolarWinds's public-facing security statement?
A. No, it would not.
Q. And why do you say that?
A. Because, you know, the -- you know, when I -- as we read the security statement, there's no specific prohibition about password sharing.
Q. So if I could ask you to look back at the security statement, Exhibit 5.
A. Uh-huh.
Q. You have that in front of you?
A. Yes.
Q. Okay. And the page ending in 337108.
Do you see that?
A. Yes, I do.
Q. And under "Authentication and Authorization," the first sentence says, "We require that authorized users be provisioned with unique account IDs."
Do you see that?

A. I do.
Q. In your mind, does that statement prohibit the sharing of login information between employees?
A. No.
Q. And why not?
A. Because, I mean, it's talking about provisioning, not how people use their IDs.
Q. And just so I'm clear, nothing in SolarWinds's security statement precludes employees from sharing their logins and passwords with each other?
A. You know, as we just discussed, the fact that authorized users are provisioned with unique account IDs is what the security statement says, and there's nothing in there -- nothing in the security statement about shared passwords.
Q. All right. In the email above in the thread, that same page that we're at --
A. Sorry. I'm just sorting my documentation.
Q. -- exhibit -- yeah, Exhibit 13.
A. Yeah, I'm just trying to get the other documentation out. Okay.
So we're -- I'm back to the point we

were at where -- like, the last email. So, yeah, I'm --
Q. Okay.
A. Yep.
Q. And the email above --
A. Uh-huh.
Q. -- there's one from Chris Day.
Do you see that?
A. Yep.
Q. And he writes, "Hello. Highlighted item needs to stop immediately. Under no circumstances is development to be done in production. If that impacts deliverables, please let August know. This is a significant security and SOX violation."
Do you see that?
A. I do.
Q. Do you agree with Mr. Day's statement that under no circumstances is development to be done in production?
MR. TURNER: Objection to form.
THE WITNESS: Not necessarily. I don't -- you know, I don't know the -- I mean, the context, you know, of -- in which he was writing this email.

But I don't -- I don't generally agree that under no circumstances is development to be done in production.
BY MR. CARNEY:
Q. Why do you say you don't know the context in which he was writing this email?
A. I mean, he's urgently responding to this initial email. You know, he -- I think he's showing urgency around, you know, a situation which he wants to get control.
You know, that's what I know about the context of this.
Q. Okay. And, in fact, in your report, Exhibit 1, starting at paragraph 122 --
A. Uh-huh.
Q. -- don't you write several paragraphs about this particular incident that Mr. Day is discussing?
A. Right. No. I have a lot of context about the incident as a whole. I think the point I'm making is any given email -- you know, I don't know what he was doing at that time of day and why he chose the language that, you know, is here, which, again, I disagree with, because, you know -- you know, there's elements of this that

show urgency.
So I don't know what was happening to Chris Day at that time when he decided to write this email this way.
Q. When Mr. Day said that "This is a significant security and SOX violation," do you agree with him?
A. The notion that "significant," I don't agree with.
Q. Why not?
A. This was, you know, a minor incident. You know, and -- you know, as they went through the process, it was -- I'm just gonna check and make sure I got the right word, but I believe that the chief -- you know, the head of information security, Tim, you know, said he thought the risk was low.
And so, you know, again, I don't think it's a significant security violation.
Q. Did you ever talk to Chris Day?
A. I did not.
Q. Did you ask to talk to him?
A. I did not.
Q. What do you understand the statement -- well, first of all, let me back up a

second.
Do you agree that it's a SOX violation?
MR. TURNER: Objection to form and foundation.
THE WITNESS: You know, I don't know all the specific provisions of SOX. I know pretty deeply that the provisions that relate to information security, you know, shared passwords, may be identified as a specific SOX violation, you know, in which case, you know, that would be a violation, yes.
BY MR. CARNEY:
Q. Well, and just to be clear, the highlighted portion that he's referring to is the development being done in production, right?
A. Right. But that doesn't necessarily mean that the violation is -- you know, is that element of what he's highlighted that Chris Day is talking about.
Q. Well, and just for context, he says in his email, "Highlighted item needs to stop immediately," right?
A. Yes. Because Chris's email says, "The highlighted item needs to stop immediately."

Q. And so when he's saying, "This is a significant security and SOX violation," he's referring to development being done in production environment, right?
A. Yes. It does appear --
Q. Okay.
A. -- so.
Q. And were your earlier responses to my questions reflecting that, or were they reflecting the password sharing issue?
MR. TURNER: Object to form.
THE WITNESS: Yeah, well, in general, I don't agree that it was a significant security instance.
I don't know which aspect of this specific minor incident he's referring to, the SOX violation, you know, you did just read that, you know, the email refers to development.
May -- he may have been referring to that in terms of a SOX violation --
BY MR. CARNEY:
Q. Okay.
A. -- which is not, you know, necessarily an information security violation, because the SOX is a -- you know, a control structure around --

like, the safety of financial controls.
Q. All right. And so you -- just so we're clear, you don't think either the sharing of the passwords or the development being done in the production environment were significant security issues?
A. You know, in this instance, no.
MR. CARNEY: A couple more questions on this, and then we'll take a break.
MR. TURNER: Thank you.
THE WITNESS: Uh-huh.
BY MR. CARNEY:
Q. Do you agree that not sharing passwords is a cybersecurity best practice?
A. Yes. Yeah.
Q. Okay.
A. It's a best practice, because humans tend to want to do things that are easy. And the type of practice that requires constant attention that occurs quite often, but it's not -- you know, it's not practice that we wanted to have happen in a security practice.
MR. CARNEY: Okay. We can take a break now.
THE WITNESS: Okay.

THE VIDEOGRAPHER: The time right now is 4:11 p.m.
We are off the record.
(Whereupon, a recess was taken at 4:12 p.m.)
THE VIDEOGRAPHER: The time right now is 4:28 p.m.
We're back on the record.
BY MR. CARNEY:
Q. All right. Dr. Rattray, before we broke, we were looking at Exhibit 13. I just had one --
A. Oh, yeah. Okay.
Q. -- the email --
A. Uh-huh.
Q. And I just want to ask you: You had mentioned that when we were talking about Chris Day's email in particular --
A. Right.
Q. -- that you didn't know what was happening to him that day.
What did you mean by that?
A. You know, I think as I mentioned, there was a lot of urgency in this email. You know -- you know, that -- actually, I sort of see

this email, you know, in a very good way in terms of just overall SolarWinds security practice where, you know, the technology leaders, you know, over and over, again, you know, see it imperative to, you know, highlight things that are security -- you know, potential security issues and, you know, be clear like a coach is clear in practice that if you miss a block, you really shouldn't do that in a game.

So, you know, I don't know whether the urgency in the email is him seeking to be a good coach or, you know, a day where he had a lot going on and, you know, wanted to get this, you know, urgency delivered quickly. This is a pretty short email.

Q. So I understand, is it your view that with most emails, you sort of need to know what was going on with the person's day to be able to understand them or to rely on them?

A. You know, I think this is one of the reasons why emails like this are not great sources of assessment of security -- you know, the presence of the -- you know, the practices outlined in this securities statement.

You do need context for emails to

understand, you know, what -- you know, what was happening, you know, in -- and it's very difficult to get that context.

So, you know, in typical industry practice, you know, you may -- you may use, you know, artifacts that are found in emails, but you're really not looking at this sort of chat-type email as the assessment of a presence of a practice.

Q. Okay. And you just -- you used an analogy about missing a block during practice and being told not to do it during a game.

Does that -- does that apply here? Was this practice that we're talking about, or was this the game?

A. You know, I don't think this was that -- you know, was not a significant security incident. You know, the ongoing, you know, practice of security, you know, requires encouragement, you know, in an ongoing basis, right?

So, you know, that was just an analogy to sort of talk to why the urgency might be here. I don't have the context for this statement.

Q. Okay. Sir, if I could ask you to

please turn to paragraph 212 of Exhibit 1 of your expert report. And I'll get you a page number. My outline just has the paragraph numbers. That's why it takes me a while.

A. [Speaking sotto voce].

The paragraph again? I could probably just go right to the paragraph.

Q. It is 212, which was on page 116.

A. Okay.

Q. And you're discussing a document that Mr. Graff cites relating to threat modeling. I have the document right here if you need to see it.

And just -- to let you know, I'm not trying to hide documents from you. I'm just trying to move this along. But if you need the document, I got it.

A. Uh-huh.

MR. TURNER: I would prefer if you.

(Simultaneous unreportable crosstalk occurs among parties.)

THE WITNESS: I think that's probably a good idea.

(Whereupon, Exhibit 14 is marked for identification.)

BY MR. CARNEY:

Q. Okay. So in paragraph 212 of your report, you're discussing a document that Mr. Graff cited, and in Footnote 358 of your report, you cite to the document.

And so what I've handed you that's been marked as Exhibit 14 is that document. And, for the record, it has Bates stamp SW-SEC-00166790.

And in the paragraph in your report, you state sort of about halfway down through that paragraph in 212, "The authors who wrote this assessment who are not deposed may have had in mind a formalized type of threat modeling that they wanted to be done rather than meaning to say that no type of threat modeling was being done in any sense."

Do you see that?

A. Yes.

Q. Have you seen any document indicating that the people who wrote "no threat modeling or analysis is performed as part of any process except MSP backup engineering" meant something other than no threat modeling or analysis is performed as part of any process?

A. That was a pretty complex question.
Q. Sure.
A. Can you restate --
Q. Sure.
A. -- it?
Q. I'll break it down for you.
Paragraph 212, you say that Mr. Graff cites a notation in this assessment --
A. Yes.
Q. -- Exhibit 14, that says no threat modeling or analysis is performed as part of any process except MSP backup engineering, right?
A. Yes. I see that, yep.
Q. And then you say that it's -- you go on to say, "It's unclear exactly what was meant by the remark in the document," right?
A. That's right.
Q. And you also go on to say that the authors who wrote this assessment, they may have had in mind a formalized type of threat modeling that they wanted to be done rather than meaning to say that no type of threat modeling was being done in any sense.
I wonder, what is the basis for your statement about what they may have had in mind.

A. You know, well, it starts from the discussion that we had, you know, I think at the beginning, you know, of today, which is, you know, "threat modeling" is, you know, a broad term.
And, you know, as we've discussed during the course of the day, you know, I see evidence, you know, that threat modeling, you know, existed in SolarWinds's practice noting that threat modeling is not part of the securities statement.
But, you know -- you know, I did sort of look at the SolarWinds practices to the extent that they, you know, evidenced threat modeling, and I find that evidence there.
So because of that, you know, I was -- you know, I spec -- you know, speculated that they may have a formalized view of threat modeling, because I -- what they found was in the face of what I saw related to the existence of threat modeling, you know.
And I reviewed the -- the FSRs for those specific, you know, products or applications just the fact that there was an FSR is evidence of threat modeling in my mind.
So that was why I thought that they

might have a more formalistic view of threat modeling.
Q. And what would a formalistic view of threat modeling entail?
A. You know, again, because I don't -- you know, I see it broadly. You know, I've seen, you know, at times detailed descriptions of threat modeling processes.
You know, that maybe, again, they were looking for a checklist around, you know, the performance of threat modeling specifically or the production of specific threat modeling artifacts.
Which, again, there are processes that exist that cause that to happen. But, you know, it's -- as discussed, you know, multiple times, I don't see that as sort of the general industry approach for threat modeling.
It's more a broad set of activities related to identification of security risk, taking that into account as you do software development.
Q. So specifically related to MSP products, which this exhibit that we were looking at is discussing Exhibit 14 --
A. Uh-huh.
Q. -- what, if any, documents did you

review regarding threat modeling in MSP products?
A. Well, you know, as stated in my report, I looked at the FSRs for the software releases for the three cited, you know, RMM, backup and N-Central.
And, you know, they show that the development teams were doing threat modeling, you know, identifying risks to software and developing mitigation.
So that was the documentation that I used in this specific case.
Q. Okay. So let's take a look at that then.
If I could ask you to turn to page 114, paragraph 210 of your report.
A. Uh-huh.
Q. And you state that, "I've also seen evidence of threat modeling and FSRs that I've reviewed. The FSRs have sections addressing security design considerations with such headings as proactive review of all FAS, high-level design documents, documents with security design implications for security-related features identified by teams."
Do you see that?

A. Yes.
Q. So the first quote that you have where it says, "Proactive review of all" -- and this is in all caps, "FAS," and then parentheses, "(high-level design documents,)" you cite to -- you have Footnote 346, and you cite to a document.
Do you see that?
A. Yes.
(Whereupon, Exhibit 15 is marked for identification.)
BY MR. CARNEY:
Q. And just, for the record, you've been handed what's been marked as Exhibit 15. And this is the document that you cite in Footnote 346, paragraph 210, and the Bates stamp is SW-SEC-SDNY_00069825.
First of all, what does -- in this sentence that I just read, "Proactive Review of All FAS High-Level Design Documents," what does FAS mean?
A. I don't know. I do not know what that -- that breakdown of that acronym is.
Q. And would you agree that under "Proactive Review of All FAS High-Level Feature Design Documents," which is on the first page of

this document --
A. Uh-huh.
Q. -- there's an empty table?
A. You know, in this case, the table is empty. But the statement is about, you know, the fact that FSRs are asking the teams to, you know, look at, you know -- you know, design documents in light of security.
The first statement of paragraph -- or sorry, yeah, the first statement of paragraph 210 is to the point where -- to the point that broadly you have threat modeling is about bringing in security to design considerations.
And the point being made is -- it's actually the second sentence, that the FSRs have -- are as templates have sections that are, you know, asking -- you know, the teams in terms of the security element of their, you know, software -- yeah, the security -- yeah, security element of this software development to consider things.
In any given instance, it -- you know, I'm not trying to say that, you know, every FSR needs to, you know, have implementations of, you know, the headings that are in the FSR.

The point here is that this FSR process is an element of, you know, them having generally threat modeling.
Q. Okay. So, first of all, this document is the one document that you cite related to proactive review of all FAS high-level design documents, right?
A. Yes. This is the document.
Q. Okay.
A. Yeah. I cite it as showing that FSRs have headings, and the heading is in the document.
Q. And so is it fair to say that you're relying on the heading on the document and not the substance of any design review that was done, right?
MR. TURNER: In this particular case?
MR. CARNEY: In the one example that he selected, yes.
THE WITNESS: Yeah, the -- I mean, you know, the sentence is not intended to, you know, look at any of these specific FSRs as -- you know, any of these specific FSRs.
It's to make the point that the process of final security reviews included design considerations, which is part of, you know, a

broad conception of threat modeling, which is not even in the securities statement.
BY MR. CARNEY:
Q. Okay. And so -- but would you agree, that given there's an empty table here, that this particular document does not support the statement that SolarWinds's developers conducted proactive reviews of all FAS documents?
MR. TURNER: Object to form.
THE WITNESS: No. I mean, because the simple point being made in paragraph 210 is the FSR process, you know, included, you know, callouts to look at these things. The sentence was never to look at the -- the specific implementation against a specific, you know, app -- application.
Again, it's just making the general point that they had a strong FSR process, and that that -- you know, also meant that they were -- you know, especially because of the way they implemented it, they were doing threat modeling.
(Whereupon, Exhibit 16 is marked for identification.)
BY MR. CARNEY:
Q. All right. Doctor, I've handed you --

if you look at the next sort of part of that sentence, it refers to -- in paragraph 210 of Exhibit 1, first to "documents with security design implications," and there's a Footnote 347.
Do you see that?
A. Yes.
Q. Okay. And so what you've been handed as Exhibit 16 is the document that is cited in Footnote 347.
MR. CARNEY: And, for the record, that's SW-SEC-SDNY_00055006.
BY MR. CARNEY:
Q. Do you -- where it says "Documents With Security Design Implications or Data Privacy Concerns" at the top, do you see the table underneath that?
A. I do.
Q. And that table has -- appears to have links to two documents?
A. That's correct.
Q. Have you been able to access either the documents that these links point to?
A. There was no need for me to access either of those documents.
Q. And why not?

A. Because as we were just discussing with the heading proactive review of all FAS high-level design documents, that the heading documents with design implications was simply to illuminate that the FSRs have, as a -- as templates, you know -- you know, look at, you know, security as a feature in design.
And, you know, call out for development teams, because they will go through the FSR process to look for the presence of these things.
As I said in the last conversation around the proactive review of all FAS high-level design documents, the intent of that sentence was never to look at a specific, you know, FSR, you know, as evidence of implementation of, you know, threat modeling.
It was to show that the FSR process hit the things that threat modeling, you know, calls for.
Q. Okay. So the documents in that table, do you know whether they relate to security design implications versus data privacy concerns?
A. I feel like I just answered that question. You know, I answered that I didn't look

at the documents for the reasons that that was unnecessary.
Q. Let me ask you: Outside of litigation when you're assessing the cybersecurity of a company, would it be your practice to rely on the title of a section in a document versus looking at the underlying documentation?
MR. TURNER: Object to form.
THE WITNESS: In terms of, you know -- can you repeat the question?
BY MR. CARNEY:
Q. Sure.
I'm just -- I'm trying to understand this -- you know, you talk about how Next Peak does this cybersecurity --
A. Uh-huh.
Q. -- assessments, and I'm wondering if the concept of looking at a heading in a final security review without looking at the underlying documentation is consistent with the sort of non-litigation cybersecurity assessments that you perform at Next Peak?
MR. TURNER: Object to form.
THE WITNESS: That -- you know, this -- we're talking about a specific sentence

where I look at the presence of headings in documents.
I've -- you know, as we've talked about, looked at over 50 FSRs, right? There was a simple point being made here that the FSRs, you know, do lead a security team through a process that includes, you know, things that, you know, you would expect if you were -- you know, to see if threat modeling.
So, you know, this -- again, was a sort of a specific assessment of implementation of threat modeling for an application.
This was the articulation of the fact that the FSRs clearly called at the process level for doing this. So this is just one of many elements of, you know, my overall assessment that threat modeling was occurring.
Again, something that was not present in the securities statement, but that I do believe, you know, the evidence in total, not this sentence only, you know, clearly indicates that they were doing.
BY MR. CARNEY:
Q. Okay. In that same paragraph 210, you say, "Some of the FSRs also include design reviews

by the architecture team further reflecting consideration of security at the design stage."
Do you see that?
A. Yes.
Q. You didn't add a citation to that sentence, did you?
A. I did not.
Q. Okay. Do you recall which FSRs you had in mind here?
A. I don't recall the specific FSRs.
Q. And have you been able to look at any design reviews by the architecture team?
A. It would be similar to the -- the answer to the previous question. That was, you know, not the point of this paragraph as a whole.
It's to the point that the FSR process includes steps, and at times, you know, included, you know, this step, design reviews by an architecture team.
You know, my -- my approach is similar to what's used in the industry. You're not trying to check, you know, every -- you know, every implementation down to the specific, you know -- the specific -- you know, the follow-through on every single specific FSR.

The FSR process at the level of the security statement, you know, demonstrates what people reading that security statement would expect from SolarWinds.
Q. Okay. So in reviewing the FSRs, you assessed whether SolarWinds had the opportunity to do threat modeling, but not whether they actually did threat modeling, right?
A. No. You know, I looked at a lot of FSRs. The FSRs, you know -- you know, show activity that falls in, you know, the conduct of threat modeling.
Again, you know, threat modeling is not part of the securities statement, but there's no reason to believe that the steps that are outlined in the FSRs in the documentation that is, you know -- you know, present -- you know, the lengths of the documentation present in the FSRs, you know, would not have occurred, right?
There's just every reason to believe these FSRs are -- you know, the FSR process itself, you know, threat modeling is -- it's a strong process that there's no reason to believe that the things that are called for, you know, when they're present and the FSR didn't happen.

Q. Well, let me just see if I can break that down a little bit.
Would you agree with me that "threat modeling" is a term of art in cybersecurity?
MR. TURNER: Object to form.
THE WITNESS: Yeah, term of art is -- I'm not -- I'm not quite sure what you mean by "term of art."
BY MR. CARNEY:
Q. It has a, sort of, generally accepted meaning in cybersecurity, the term "threat modeling"?
A. You know, "threat modeling" is one of the terms in cybersecurity where there are a lot of, you know, sort of interpretations of what those words mean.
Yeah, you know, so I think a lot of people have a -- you know, different conceptualizations of what is meant when you use the words "threat modeling" in cybersecurity.
Q. In your view, is threat modeling the same as risk identification?
A. You know, threat is an element of risk. They're not synonymous, but they're -- you know, I guess I would consider them overlapping.

Q. So what's the difference between threat modeling and risk identification?
A. Well, risk identification, you know, also includes the understanding of vulnerability. You know, that's sort of classic terminology in cybersecurity regarding risk is its threat and vulnerability.
Q. Okay. Is there a difference between threat modeling and risk mitigation?
A. In general in the field or --
Q. In the cybersecurity field.
A. Yes, there's -- the two things, they are different. "Threat modeling" could be an element -- to me is a broader term of risk mitigation.
Q. Are you aware of any steps that are part of threat modeling as a cybersecurity best practice?
MR. TURNER: Objection to form.
THE WITNESS: You know -- you know, I think we've discussed this. That, you know, threat modeling is -- you know, broadly, you know, the identification of, you know, what act -- you know, actors could do in terms of threatening a specific, you know, organization.

You know, identifying those as security concerns working towards, you know -- in the case of software development, you know, that informing the software development.
BY MR. CARNEY:
Q. Okay. And I guess what I'm trying to understand as -- you know, as a layperson is -- is there, like, a typical, like, written output that you would expect to see from a threat modeling being conducted?
A. No. Not necessarily. You know, in the broad conception of threat modeling, it's -- you know, the -- in these processes, some of which are in this paragraph, you know, being present is indicative of, you know, getting the team to think about how threat affects, you know, the development in this case.
So specific artifacts, you know, are not necessarily an outcome of threat modeling.
Q. When you've been involved in threat modeling in the past, have you or a team working for you typically produced a written output?
A. You know, I've seen outputs of a formalistic threat modeling process, but that -- I've also seen teams discuss, you know, threat

and, you know, not produce a formal -- a specific output from that exercise.
Q. All right. And the times where you've seen outputs of a formalistic threat modeling process, what did that output look like?
A. You know, it could be lists of specific actors. It could be lists of, you know, threat actor, you know -- you know, approaches. But, you know, more broadly, again, the concept of threat modeling doesn't necessarily call for these outputs.
And, you know, in the case that we have in front of us, there isn't even a specific identification that threat modeling is part of what's promised in the secure -- you know, asserted to be one of the -- SolarWinds's, you know, activities in the securities statement.
Q. All right. Sir, if I could ask you to look at paragraph 211 of your report --
A. Uh-huh.
Q. -- page 115. And you have a discussion there of Mr. Colquitt's email.
Do you see that?
A. Yes, I do. I should probably, you know, look at both the email and his explanation

in the deposition, but I see -- I see that sentence here.
Q. Okay. I don't -- right now I don't want to focus on the substance so much as I want to understand your process for forming your opinions about Mr. Colquitt's email in this report.
And I'm wondering, when you are discussing Mr. Colquitt's testimony about what the email he wrote meant, were you sort of accepting it at face value, his explanation?
MR. TURNER: You mean was he assuming it was true?
MR. CARNEY: Right.
THE WITNESS: Again, I think -- I think in this case it's important, because this, you know, sentence talks both about an email and then it talks about what he said in his deposition when he wrote the email.
So, you know, in most of the sentence, you know, where -- you know, I'm looking at two sentences, but most of that is quotation.
MR. TURNER: I think the question is simply whether you were assuming Mr. Colquitt was truthful in his testimony.

THE WITNESS: I believe he was truthful in his testimony, yes. I mean, that is an assumption in the way I wrote my -- you know, my report.
BY MR. CARNEY:
Q. And so specifically I want to focus you on the sentence in the middle of paragraph 211 were you write, "In saying that, 'We are just barely beginning to understand how teams are going to be doing this activity,' he was not, 'talking about doing a threat modeling itself,' but was rather talking about how teams were going to be documenting that activity."
For purposes of that sentence that you wrote there, is it fair to say that you just relied on Mr. Colquitt's explanation of what his email actually meant?
A. You know, in terms of SolarWinds's conducting threat modeling, I wasn't, you know, solely reliant on this statement. We've talked a lot about, you know, the evidence I relied upon to find that, you know, threat modeling was occurring in SolarWinds.
As we just stated, I believe, you know, in terms of what I quoted, I believe he was

telling the truth in his deposition.
Q. And my question is: Have you seen any independent evidence to support Mr. Colquitt's statement that he was not talking about doing threat modeling itself but simply was talking about how teams were going to be documenting threat modeling?
A. Again, you know, I just want to make sure that I'm, you know, correct about this. But if we had, you know, the timing of the email, you know, that would help.
Because, you know, as I've said over and over again, the -- one of the primary sources of, you know, my finding that threat modeling was occurring is the presence of the -- the FSRs.
You know, again, those were put in place just prior to the relevant period. But I -- you know, I don't remember the exact timing of this statement.
But, you know, those would certainly be independent of his assertion that they were not just talking about, you know -- you know, that they were doing threat modeling, and that what he was talking about was documenting the activity.
Q. All right. So if the first sentence

of 211, you say, "With respect to Mr. Colquitt's email, it appears to me Mr. Graff takes this email out of context." So let's stop there.
What do you mean that he took the email out of context? What's the context?
A. Well, I mean, the context is explained by Mr. Colquitt in his deposition.
Q. Okay. Is there any other context?
MR. TURNER: Object to form.
BY MR. CARNEY:
Q. That you feel Mr. Graff failed --
A. I -- I -- you know, I'd like to look at the email.
Q. So I don't have a copy of the email, because you quoted most of it in your report. But --
A. Yeah, I don't -- I don't have specific memory of the entire email.
Q. Okay. Did you ever interview Mr. Colquitt?
A. I did not.
Q. Dr. Rattray, is it fair to say that it is your opinion that SolarWinds did not 100 percent of the time conform to the cybersecurity practices described in the security

statement?
MR. TURNER: Object to form. And foundation.
THE WITNESS: As my report, you know, states, basically no security practice can, you know, conduct a perfect implementation of the set of things that are listed in the securities statement.
Perfection is -- you know, is not the goal here. It's not the expectation of readers of the security statement.
BY MR. CARNEY:
Q. Fair enough. And I'm just trying to -- really right now I'm just trying to understand your opinion.
A. Uh-huh.
Q. Is it fair to say that it's your opinion that whatever lapses there were, were not pervasive or frequent at SolarWinds?
A. I think that's fair. There were -- you know, these were not pervasive, you know, systemic lapses, you know, to the extent that any of them existed.
Q. And is it fair to say that it's your opinion that a small number of lapses over a

multiyear period do not render this assertions in the security statement untrue?
A. Can you just repeat one time for me?
Q. Sure.
Is it fair to say that it's your opinion that a small number of lapses over a multiyear period do not render the assertions in the security statement untrue?
A. Excuse me. It's fair to say that, you know, the security statement calls for, you know, the presence of, you know, activity and practices.
And that, you know, given the nature of cybersecurity, you.
(Stenographer asks for clarification.)
THE WITNESS: You will not achieve perfection, you know, in the implementation of those practices. You know, and so -- you know, that's -- that's sort of, you know, my opinion. And, you know, that's what -- you know, we're looking for here.
I don't think any reader of the securities statement is looking to that statement to sort of hold -- you know, hold SolarWinds to its -- to its -- you know, to perfection in the execution.

BY MR. CARNEY:
Q. So is there a number of lapses that, in your opinion, would render the assertions in the security statement untrue?
A. You know, that is not the way we look at, you know, sort of evaluating things like, you know, the presence of controls or activities, like, laid out in the security, you know -- in the security statement.
So you have -- the determination is not numerical. I mean, I haven't done very -- you know, done large numbers of assessments and read large numbers of assessments on things like access controls.
There's not a quantification, you know -- you know, involved in security assessment and, you know, evaluating the presence of practices.
Q. So is it fair to say that there's a qualitative aspect of such an assessment?
A. Yes, it is fair to say.
Q. And so, for instance, if a company enforced their cybersecurity controls 99 percent of the time, but the 1 percent of the time they didn't was for the most critical systems, that

would matter in a cybersecurity assessment, right?
A. You know, in terms of the assessment of the security statement, which is not about sort of -- it's about the presence of processes, right?
It says SolarWinds's -- you know -- you know, I don't want to -- to the -- you know, it says -- I just want to be precise -- you know, that SolarWinds is conducting activities.
You know, the magnitude -- it does not discuss, you know -- again, I have to take a quick look, but I do not think it discusses, you know, the -- the magnitude of anything.
It discusses, you know, activities that SolarWinds conducts. So in terms of assessing this statement and what it asserts, the magnitude of any specific, you know, problem that might be identified actually is not relevant to the securities statement.
Q. This is a hypothetical --
A. Uh-huh.
Q. -- but can you think of a type of cybersecurity mistake that is so serious that even one instance of it would indicate a major flaw with an organization cybersecurity controls?
MR. TURNER: Object to form.

THE WITNESS: Please repeat the question.
BY MR. CARNEY:
Q. Sure.
Can you think of a type of cybersecurity mistake that is so serious that even one instance of it would indicate a major flaw with an organization's cybersecurity controls?
MR. TURNER: Object to form.
THE WITNESS: You know, I'm just trying to think of -- the answer is generally, no, right? Because, you know -- you know -- or maybe we have to talk about what "flaw" means.
But, you know, cybersecurity is difficult, and perfection is basically impossible to achieve. So the fact that there's a flaw, that does not mean that -- you know, the organization -- you know, again, we're in a hypothetical here -- isn't actually good at that control, right?
You know, I cite the example, you know, in my report of an error that occurred in the World Series by a fielder that hadn't had any errors, right? So that was a pretty serious flaw but, you know, like, flaws happen, right?

So I don't think it's -- you know, certainly a singular incident isn't sort of a reflection of, you know, on -- isn't a reflection on a judgment related to the -- you know -- whether a control structure is there or, you know -- yeah, is there.
BY MR. CARNEY:
Q. And just for the record, that reference to that error was a personal affront to me, and it was painful so soon after the World Series, but that's --
A. I understand.
Q. -- neither here nor there.
So let me give you a hypothetical. Let's say -- this is a hypothetical. U.S. government accidentally leaks the passwords that are needed to use the nuclear weapons, like the -- what is it? -- the biscuit?
A. It's not a biscuit. But the briefcase.
Q. The briefcase?
A. Briefcase moves around with the President.
Q. Got it.
A. Yes.

Q. And it happens only once.
Would you agree that despite this mistake not being frequent, it could still indicate a significant issue with the government cybersecurity controls?
MR. TURNER: I'm going to object to form.
A "significant issue," do you mean a consequential one or do you mean a pervasive one?
BY MR. CARNEY:
Q. Well, you can answer.
Significant in that it's important.
A. Yeah, I mean, you know, the distinction being made, you know, "significant" can be -- you know, an issue of magnitude, which is -- we were just discussing, you know, a singular mistake doesn't, you know, mean a control -- control process is not strong.
You know, mistakes get made. You know, its magnitude could be grave in a single instance, but it's not -- you know, not an indication of a pervasive failure of, you know, any given process or control.
Q. If the military attache that was supposed to be guarding that briefcase routinely

left it in the restroom but only one time did someone take it, would that be -- could that be indicative of a systemic problem, even though it was only leaked that once?
MR. TURNER: Again, I'm sorry. But he routinely left it unattended in the restroom? That was your...
MR. CARNEY: Right.
BY MR. CARNEY:
Q. But it was only stolen once.
MR. TURNER: But it was done routinely?
MR. CARNEY: Right.
MR. TURNER: Okay.
THE WITNESS: Again, we're talking about -- obviously we're talking about --
BY MR. CARNEY:
Q. A different hypothetical?
A. -- a hypothetical, right, and actually knowing people that have been responsible for carrying that briefcase personally. You know, there's a lot of process that goes into avoiding, you know, routine misbehavior like that.
You know, because it's a -- an error would be grave. So, you know, if -- you know, if

the -- the bad event was the result of clearly numerous indications of, you know, misapplication of the -- the control, you know, you would want to be reviewing that, you know, when you had the incident.
You know, that's my sort of perspective on that hypothetical.
Q. But in the original hypothetical, if it was -- only happened one time, that wouldn't warrant the review of the controls?
A. I didn't say it wouldn't warrant a review.
Q. And it could possibly be evidence of a serious problem with the controls, right?
A. Yeah. Again, you would look at the context. You know, in most cases -- and, again, we're talking very hypothetically, so whether this applies to SolarWinds or not, it largely doesn't apply to the security statement for the reasons I've said, which is the security statement is about the presence of activities and programs.
You know, if a serious error was to occur, there would be a review. You know, yeah. So, you know, that's generally what happens in, you know, these types of processes like your

hypothetical.
Certainly I am sure that if the briefcase was, you know -- you know, lost, it would be a very significant review of why that occurred.
Q. And the briefcase is the football, right, and the biscuit is the thing the President carries, right?
A. The briefcase is sometimes referred to as a football, right, you know.
Q. So, sir, if I could ask you to look at paragraph 104. This is the bottom of page 57, and Exhibit 1 and carries over to page 58.
A. I did it again [speaking sotto voce].
MR. TURNER: Do you just want to give him a chance to read it?
MR. CARNEY: Yeah.
THE WITNESS: So we're gonna -- we're gonna discuss material in paragraph 104?
BY MR. CARNEY:
Q. Yes.
A. Okay.
(Pause for reading/reviewing.)
A. Okay. I would have looked through paragraph 104.

Q. Okay. At the end of paragraph 104, the last sentence you say, "Nor does Mr. Graff identify any benchmark for an expected or acceptable error rate against switch to judge implementation of SolarWinds's controls even though he acknowledges repeatedly that errors and lapses occur in any cybersecurity program."

A. Right.

Q. I want to ask you: Is it your opinion that Mr. Graff should have identified an acceptable error rate against which to judge the implementation of SolarWinds's controls?

A. Yes, it is. Because Mr. Graff is making assertions around pervasiveness and systemic issues, which inherently involve, you know, a -- you know, some sort of expectation of what constitutes pervasive versus systemic.

Q. Okay. And you yourself did not calculate acceptable error rate, did you?

A. Yeah, because we were doing very different things.

Q. And in your concept of the acceptable error rate, what is the numerator in the rate?

A. I didn't make any assertions around pervasiveness or systemic. And I -- and I -- so

for the places where Mr. Graff is asserting that something is pervasive or systemic, I'd have to look at that specific situation.

But, you know, it certainly wasn't within, you know, the -- the task I had at hand to determine those rates.

Q. Right. And I'm just trying to understand the error rate that Mr. Graff -- that you feel he should have calculated.

What would be the numerator in that rate that he should have calculated?

By that I don't mean the actual number. I mean what category of items would go into the numerator?

A. Again, this is completely contextually dependent.

MR. TURNER: I think you might be talking past each other.

Are you saying, like, what is the numerator?

MR. CARNEY: Right.

BY MR. CARNEY:

Q. What is in the formula?

MR. TURNER: If errors are systemic, what is the -- what is the numerator?

MR. CARNEY: What is the numerator, what is the denominator for the --

THE WITNESS: Yeah, I don't know for a given control.

(Simultaneous unreportable crosstalk occurs among parties.)

THE WITNESS: If the denominator is tens of thousands of, you know, instances of occurrence, how many errors, you know -- I don't -- again, I can't in this question say if that number is 10, 100. You know, those sorts of things.

And what that number is, is very dependent on what control and situation. Even the factors that go into determining -- determining if it's 10 or 100.

MR. TURNER: Can I try?

Go ahead if you want. I think I know what you're getting at.

BY MR. CARNEY:

Q. Yeah. And I'm not looking for you to quantify it or give me a number between 1 and a million.

A. Right.

Q. I just want to know what types of

activities go into the numerator versus into the denominator in calculating that error rate? Is it incidents go into the numerator?

A. Controls have such -- you know, there are a lot of controls, and even the data that is used for those controls varies widely. I don't know what goes into the numerator for any -- unless we talk about a specific control.

Q. All right. So is it fair to say that the error rate that you say that Mr. Graff should have calculated, you yourself don't know how that would have been calculated?

A. No. That's not what I said. I said you need to give -- you need to talk to me about a control, and I'll talk to you about how -- how I might go about it theoretically given that that was not the task that I had at hand.

Q. Okay. Let's use passwords then.

So how would you calculate an error rate for the password policy?

A. You know, again, you know, you would look at, you know, how many instances of -- again, the -- you know, the password policy, you know, has different stages.

But let's just say the number of times

you issued a new employee password and you would have -- you know, you would seek to devine a denominator -- you know, you would -- data that gave you sort of a denominator that -- to that.

And then, you know, if you were going to say it was systemic, you would work at, you know, probably through a structure, you know, of -- you know, interaction of, like, what percentage -- I mean, we have risk metrics all the time.

So you sort of set thresholds for, okay, you know, 5 percent error rate, you know, starts to get on a -- you know -- on a risk reporting, you know, ledger, right?

So, you know, it is certainly possible and happens quite frequently in terms of measuring control implementation that metrics are put in place that include determinations and numerators that are relevant to the denominators.

MR. TURNER: Just to -- I just want to be -- just to be clear.

THE WITNESS: Hopefully -- I'm trying to answer the question.

MR. TURNER: Just to be sure, by "numerator," he's talking the errors, like the

noncompliant passwords --

A. Right-

Q. -- and the total number --

(Simultaneous unreportable crosstalk occurs among parties.)

(Stenographer requests one speaker at a time.)

THE STENOGRAPHER: It's not clear for the record.

MR. TURNER: Do you want me to repeat?

THE STENOGRAPHER: Please.

MR. TURNER: Just I want to make clear, I think by "numerator," we're talking about the number of noncompliant passwords, the denominator would be the total number of passwords in that particular example.

THE WITNESS: Yeah, I'm good -- I agree with that.

MR. CARNEY: Okay. All right. It's been an hour, I think.

We can take a break. Thanks.

THE WITNESS: Okay.

THE VIDEOGRAPHER: The time right now is 5:27 p.m.

We are off the record.

(Whereupon, a recess was taken at 5:27 p.m.)

THE VIDEOGRAPHER: The time right now is 5:48 p.m.

We are back on the record.

BY MR. CARNEY:

Q. All right. Dr. Rattray, I'm going to ask you a little bit about password protection.

Do you agree that, sort of, after the fact, incident response cannot fully compensate for inadequate password protection?

A. I think it's very contextual.

Q. Okay. Well, all right. Do you agree that poor password security can lead to breaches that happen too quickly or too stealthily for incident response to mitigate them effectively?

MR. TURNER: Objection to form.

THE WITNESS: You know, again, we should look at the specific context. You know, again, these are a very, sort of, abstract question.

BY MR. CARNEY:

Q. Right. And in fairness, you're an expert witness, so I'm --

A. Uh-huh.

Q. -- permitted to ask these kind of abstract questions.

A. Okay.

Q. So I'm talking just at a general level, can there be situations where poor password security leads to a breach that just happens too quickly for the incident response to mitigate it effectively?

Are you aware of such situations?

MR. TURNER: Object to form.

THE WITNESS: Yeah, I mean, I think that the general proposition that a control lapse could lead to a breach that -- you know, evolved quickly, you know, it's not just password protection.

You know, other security controls, you know, could lead to, you know -- again, very theoretically, could lead to rapidly, you know, evolving situations.

BY MR. CARNEY:

Q. And what other security controls are you thinking of?

A. I'm just trying to -- I mean, almost all security controls, if they fail dramatically, can be highly problematic.

So, yeah, you know, misconfiguration on a -- you know, on a device or an unpatched system, you know, would be other types of security controls that could lead to a similar situation.

Q. Okay. And do you agree that once attackers gain valid login credentials, they can often escalate privileges and move laterally across a network in minutes?

MR. TURNER: Objection to form.

THE WITNESS: Yeah, that's not generally how it occurs. So, yeah, generally I don't agree with that.

BY MR. CARNEY:

Q. I don't think I used the word "generally" --

A. Okay. Okay. All right.

MR. TURNER: What are you asking, Chris? That sometimes an attacker can get in and escalate privileges and move laterally across a network?

MR. CARNEY: In minutes, right, yes.

THE WITNESS: Yeah, that's why I said, you know --

MR. TURNER: Is that possible? Is that the question?

know, you layer security controls, and, you know, you can have compensating controls.

And, you know, you look at those, and if you're looking at a specific situation and, you know, hopefully -- you know, you're looking to have a layered set of controls that, you know, if one doesn't work well, others compensate for that.

Q. Right. And do you agree that even if an incident response team detects a breach quickly, damage may already be done?

A. Not necessarily, right? You know, again, compensating controls that limit damage for a breach are not just incident response.

Q. Do you agree that a password leak may be used months later bypassing any immediate response efforts?

MR. TURNER: I don't even understand the grammar of the question.

But object to the form.

THE WITNESS: Could you just restate, please.

BY MR. CARNEY:

Q. Yeah, a leaked password, someone could sit on it for months and not use it until months after it was leaked, right?

BY MR. CARNEY:

Q. It happens, right?

A. Yeah. Rarely.

Q. I mean, if -- you know, if you want me to tell you -- you know, the purpose of the -- I'm not required to --

A. Uh-huh.

Q. -- but the -- isn't it true that after the fact, incident remediation is not a substitute for strong password protection, right? Would you agree with that statement?

MR. TURNER: Objection.

THE WITNESS: Um --

MR. TURNER: Objection to the form of the question.

THE WITNESS: I wouldn't, because security controls are not considered substitutes for each other.

BY MR. CARNEY:

Q. Right. So you couldn't just say, we have quick remediation procedures, therefore, we don't need password protection, right?

A. In my estimation, you know, I never heard a conversation where that sort of consideration has ever come up. So I just -- you

A. Yeah, theoretically that could happen.

Q. And is it fair to say that you accept that at least in one incident in 2019, a security researcher reported finding a SolarWinds password contained in the code repository that had accidentally been made publicly available on GitHub?

A. Yes, I remember that specific situation.

Q. And just so I understand your opinion about that, is it your opinion that this incident was quickly remediated after the external security researcher reported it?

A. That's my understanding is it was quickly remediated.

Q. And why does it matter that it was quickly remediated after the discovery?

A. You know, I think -- you know, we should probably look specifically at how I phrased --

Q. Sure.

A. -- phrased that, because I think you're asking for -- you're asking me --

Q. Sure.

A. -- for why I said that, right? So can

we point -- can you point me to where this is discussed?
Q. Sure. I think it's in paragraph 132 of your report. Exhibit 1.
A. Uh-huh. Yeah, we're in -- that's the right area.
Q. Page 72.
A. Yes. So I'm reading, yeah, paragraph 132.
And, you know, is the question why I mentioned the fact that the -- the incident was remediated immediately after?
Q. Well, we can start with that.
Why did you mention it?
A. Because -- yeah, I mean -- in numerous places in Mr. Graff's report, he talks to -- about the severity of incidents, you know, and the fact that, you know, this incident was, you know, remediated immediately, you know, is relevant to, you know, the judgment of whether it was, you know -- you know, the magnitude of the risk was high.
It also, you know, shows more generally that -- you know, SolarWinds as a security practice, you know, again, more

negative consequences here.
So, you know, the fact that they -- I actually think that the fact that they remediated it quickly is just evidence that they -- they were constantly looking for problems and acting quickly when they can.
I actually don't -- you know, again, because it was another compensating control, the two layers of control quickens a response and, you know, digital signature, you know, meant that -- this incident wasn't significant.
Q. Okay. You mentioned digital signature --
A. Uh-huh.
Q. -- was that one of the compensating controls that, for lack of a better term, failed in connection with the Sunburst incident, as you understand it?
MR. TURNER: Objection to form.
THE WITNESS: No.
BY MR. CARNEY:
Q. You don't recall any aspect of that incident relating to the digital signature?
MR. TURNER: Different question.
Go ahead.

generally, you know, had layers of controls, had a series of compensating controls to deal with, you know, any singular isolated lapse like the one in this incident.
Q. Okay. And in your view as someone in the cybersecurity field, why is it important that a password leak be remediated quickly?
A. You know, I think, you know, the general practice in the field is to try to remediate any, you know, security lapse as fast as possible.
Q. All right. So we're talking about this particular --
A. Uh-huh.
Q. -- one here.
What are the consequences of not remediating it quickly?
A. You know, are you asking what -- in this specific context, what might have happened badly if they didn't have quick remediation?
Q. Right.
A. As it states in the report, it was another compensating control around digital signature that also, you know, would have -- you know, remediated the -- you know, the potential

THE WITNESS: Yeah, you know -- you know, my understanding of the Sunburst incident is, you know, the highly sophisticated Russian, you know, intelligence agency that intruded on SolarWinds got inside their software development process.
And, you know -- you know, in the distribution of that, you know -- you know, distributed software that, you know, I don't have the forensics, but probably was digitally signed. So it's a very different sort of situation.
BY MR. CARNEY:
Q. Okay. If a cybersecurity incident such as a password leak is not remediated quickly, what can happen? What are the consequences?
MR. TURNER: Objection to form.
THE WITNESS: Yeah, that is very dependent on the situation.
BY MR. CARNEY:
Q. I'm trying to understand why it mattered to you that they remediated the password leak quickly? How does that reflect on whether they were following their password practices or not?
A. As I said, you know, and Mr. Graff in

numerous cases, you know, discusses, you know -- you know, these particular incidents and makes assertions around their magnitude and severity.

And, you know, this particular, you know, callout on the compensating controls including the speed of investigation, you know, both sort of addresses the fact that this wasn't -- you know, a major or serious incident.

And more generally, you know, shows that SolarWinds had strong security practice, which would then -- you know, I mean that -- you know, in areas like password security or across the full set of, you know, activities in the security statement that this was a practice that was strong and one would expect was doing the things in the security statement.

Q. Did you review any risk acceptance forms in conjunction with your work in this case?

A. Yes, I did.

Q. And why did you review risk acceptance forms?

A. You know, in some of the incidents, a determination was made that, you know -- you know, there was a risk acceptance that, you know -- that helped address what happened, you know, or was

part of addressing what happened in the incident.

Q. Do you recall which incident?

A. I believe, but I want to confirm, you know, that this is the incident that involves the access of developers -- in the billing system or the -- the -- yeah, the -- the billing -- you know, the billing system, you know, event or, you know, situation.

Q. So doing development work in the production environment; is that fair to say?

A. I just want to make sure that I'm correct and, you know, that is one of the places that I looked at risk assessment. Pretty sure. There's a lot of detail in this case.

Q. So if you look at, I think, paragraph 123 of your report --

A. Uh-huh.

Q. -- on page 68.

A. Yeah, okay. So that's correct.

Q. So -- I --

MR. TURNER: I just want to make sure I'm looking at the right part.

What are you looking at, Chris?

MR. CARNEY: So if you look at the bottom of page 68.

MR. TURNER: Okay.

BY MR. CARNEY:

Q. So -- and I just want to ask you about risk acceptance forms generally.

A. Uh-huh.

Q. Do you agree that risk acceptance forms can show that an organization identified certain risks stemming from violation of a policy?

A. Just risk acceptance forms that -- you know, are a -- you know, the form itself is sort of the documentation of a process that, you know, if an activity is deemed risky, judgments are made about, you know, what is acceptable behavior, you know, or the acceptable path or not going forward in terms of the risk acceptance process.

And, you know, again, the form is the documentation of that process occurring and decisions being made.

Q. Got it.

And all I'm trying to understand is that -- will that form contain an assessment of the risks that you face if you violate the given policy?

A. Yeah. I mean, usually I think it does. Again, are we talking in this specific case

about this specific incident or generally? Because risk acceptance forms are per- -- you know, risk acceptance is a common way of dealing with, you know, security situations and risks.

And, again, it -- I've seen it in many different contexts.

So are we talking about a general process or the specific case here?

Q. So right now I'm asking generally.

A. Okay.

Q. And I'll ask you specifically --

A. Right.

Q. -- in a second.

So just generally I'm trying to understand, do risk acceptance forms generally show the risks that a company will face if they were to accept the given risk and violate the policy?

A. Yeah, they -- I mean, often they're not, sort of, you know, judgments on the policy as a whole. You know, they tend to be, again, context driven and situation specific.

But, you know, yes, you know, in my, you know, experience, you know, this process and those forms do identify what risks are being, you

know, considered in -- for acceptance or not generally.

Q. All right. Maybe it's easier, I'll just show you the specific example that we're talking about --

A. Uh-huh --

Q. -- here.

A. -- right.

(Whereupon, Exhibit 17 is marked for identification.)

BY MR. CARNEY:

Q. And just for the record, what you've been handed as Exhibit 17 is the native version of a document that had Bates stamp SW-SEC00168780. And it was a July 2020, RAF or risk acceptance form spreadsheet. And it was cited in Mr. Graff's report.

And I want to ask you, sir -- and just so you -- it's a sort of a big spreadsheet --

A. Uh-huh.

Q. -- just the way it's set up is that each row, if you will, spans two pages. So if you could turn to the third page.

A. So page 3 of 8 in this --

Q. Page 3 of 8 in this exhibit.

A. Uh-huh.

Q. And you'll see Row 9, the BizApps Billing DB.

Do you see that?

A. Yeah, I do.

Q. And then if you want to see the entire row, you would turn to page 4 of 8.

A. Okay. Yeah.

Q. And if you look in Column M on page 4, you see, "11/18/19. Risk reviewed and accepted by Tim Brown."

Do you see that?

A. I mean, I think -- I just want to make sure.

So I see Columns J and K. K has, you know, Tim Brown's name on Approved By. Uh-huh, yeah, if that's what the question was, the answer's yes.

Q. Okay. And then if you look at Column M, that has under "Compensating Control," there's actually a date and a notation, "Risk reviewed by and accepted by Tim Brown."

Do you see that?

A. I do.

Q. So would you agree that Row 9 of this

spreadsheet shows that SolarWinds accepted the risk that developers had write access to production data?

MR. TURNER: Generally, or are you talking about in this specific instance?

MR. CARNEY: In this specific instance, yes.

Thank you.

THE WITNESS: Yes.

BY MR. CARNEY:

Q. And do you agree that that same cell that we're looking at here, this would be Column C --

A. Uh-huh.

Q. -- states that, "APIs have write permissions which are not used or needed"?

A. Yes. I mean, this sentence has -- you know, they are using the APIs just to pull data, but those three APIs have write permissions which are not used.

Q. And do you agree that access that is not used or needed is not the least necessary amount of access?

MR. TURNER: Object to form.

THE WITNESS: Not necessarily. You

know, my understanding of this situation is the way that technology was set up, you know, at the time, you know, you didn't have a choice to have, you know -- you know, to use the technology without write permissions.

So, you know, all sort of least privilege and rule-based access is sort of in the context of, you know, what you need to do to do your job. And the developers, to do their job, needed to use these APIs.

BY MR. CARNEY:

Q. Is it your understanding that SolarWinds had a policy to separate development from production?

MR. TURNER: Object to form.

Yeah, in the network security portion, I believe of the security -- let's just check that.

BY MR. CARNEY:

Q. Of Exhibit 5.

A. Yeah. Yeah, it's in the network security portion of the security statement.

Q. And are you specifically referring to the first sentence of the second paragraph --

A. Yeah.

Q. -- where it says, "SolarWinds maintains separate development and production environments"?
A. Yes, I am.
Q. Do you agree that the risk outlined here where developers had access to production data is inconsistent with separating development from production?
A. Are we talking about the write aspect of it or some other element of this?
Q. So we are talking about the developers having read and write access to production data where they were doing their development work.
You recall this from our discussion earlier, right?
MR. TURNER: "You" here is asking -- even with read access, would be reading production data.
So I think he's asking do your questions relate to this or another aspect of --
THE WITNESS: Yeah, I mean, we're on this notion that, you know, the risk was poised because they had write access, and then we, you know, pivoted to development and production environment.

You know, as something SolarWinds -- I'm just trying to relate the two.
BY MR. CARNEY:
Q. Okay. So, well, let me break it apart then.
Do you agree that these developers had -- were performing development work in a production environment?
A. Yes.
Q. Okay. And do you agree that SolarWinds had a policy against allowing development in production environment?
MR. TURNER: Chris, are we talking about the security policy --
(Simultaneous unreportable crosstalk occurs among parties.)
THE WITNESS: Yeah --
BY MR. CARNEY:
Q. Yes.
A. And, again, SolarWinds had a network security, you know -- set in the network security portion of its securities statement that it maintains network, you know, by implication, separation of development and production network environments.

That's different than developers as people conducting activity, you know -- you know, developers inside the production environment. It's -- to my mind, an apple and an orange.
Q. So you don't believe that SolarWinds had a -- relating to your second point, a policy of preventing people conducting development inside the production environment?
MR. TURNER: Objection to form.
You're asking was there a policy beyond what's in the securities statement?
MR. CARNEY: No.
MR. TURNER: Okay.
THE WITNESS: Yeah, are you saying that the securities statement in some way obligated, you know, SolarWinds to prohibit, you know, developers from operating in the production environment? Is that --
BY MR. CARNEY:
Q. Yes.
A. -- is that the question?
Q. Exactly.
A. I don't see that language in the security statement. But, again, maybe I need to read more -- more thoroughly every sentence.

Because the network security element of it doesn't -- doesn't address the people aspect of this.
It talks about -- it's about network separation.
Q. All right. Well, so let -- let me ask you then: Do you agree as a cybersecurity professional that it is -- I'm talking about best practices here --
A. Uh-huh.
Q. -- that it's not part of a secure software development lifecycle to develop inside the production environment?
MR. TURNER: Object to form.
THE WITNESS: Again, are we talking separate from the security statement and just sort of abstractly about best practice?
BY MR. CARNEY:
Q. I'm not gonna -- I'm not gonna argue with you about what the security statement covers, so right now I just want to ask you about best practices.
You can put aside the security statement for a second.
Do you agree that it is not part of a

secure software development lifecycle to allow development inside the production environment?
A. No. I think that's a case-by-case determination based on, you know, what the business needs in terms of development. And, you know, one might seek to keep developers out of the production environment.
There's no absolute in this case, and there may be business-driven reasons to allow for developers to work in the production environment.
Q. Do you agree that "SDL, secure development lifecycle," is a term of art within the cybersecurity field?
A. Yes. It's a term of art within the cybersecurity field.
Q. And do you know which organization invented or first documented the SDL?
A. You know, again, I'm not quite sure why we're working on history at this point, but, you know, I know that Microsoft had an early role in, you know, the concept of secure -- you know, secure software development.
Q. Do you recognize Microsoft as an authority on the SDL process?
A. You know, there might -- you know, so

there are many authorities on -- you know, or many, sort of, organizations that, you know, provide advice around, you know, the conduct of secure software development.
You know, that device is used by teams, you know, in order to hopefully, you know, improve security practice, you know, generally -- you know, as a sort of general perspective on how -- how this works in the field.
Q. Have you ever read the book by Michael Howard and Steve Lipner produced by Microsoft, "The Security Development Lifecycle"?
A. I'm aware of the book, but I haven't read it.
Q. Okay. Do you recognize that book as an authority in the field?
A. As I said, I don't actually look to find authoritative sources related to secure, you know, software development.
Just, you know -- you know, practices and procedures that are, you know, advised to companies in pursuit of that -- you know, pursuit of secure software development.
But you know, the issue of an authoritative source is sort of not something that

is, you know, part of what, you know, in my practice, I'm looking for in this area, because there's plenty of good guidance.
Q. Okay. Do you acknowledge that threat modeling is a security best practice within an SDL?
A. I would say threat modeling is mentioned in, you know, that security -- you know, secure software development, you know, practices, yes.
Q. Okay. And do you agree that threat modeling is a standard practice within the SDL?
A. You know --
MR. TURNER: Wait a minute. Wait a minute. Within the SDL?
MR. CARNEY: Within an SDL.
THE WITNESS: So, yeah, we're saying, sort of, conceptually if an organization is doing software development and secure development, is threat modeling a standard?
BY MR. CARNEY:
Q. Standard practice, right.
A. You know, I don't have the data. You know, I guess if "standard" means, you know, some, you know -- some high percentage of the

organizations that do software development, you know, use threat modeling, I actually don't know whether that's a case, because there's some pretty small organizations that do software development.
And, you know, they -- they -- my sense is there's probably a lot of them that are not doing threat modeling, so I wouldn't call it a standard.
Q. Okay. Do you recall whether the Microsoft SDL book has an entire chapter on threat modeling?
A. I don't.
Q. Okay. Would it surprise you that it does?
A. No, it would not.
Q. All right. Do you agree that "penetration testing" is a term of art within the cybersecurity field?
A. Yes.
MR. TURNER: I'm just going to object to form.
THE WITNESS: Okay.
MR. TURNER: Go ahead.
THE WITNESS: I'm going too fast. Yes.

BY MR. CARNEY:
Q. And what is penetration testing, according to standard cybersecurity practices?
A. Again, the notion that, you know, there's standard practice in cybersecurity is -- you know -- you know, often really not the case. I mean, there are a lot of ways to conduct penetration testing, so, you know, I don't know that there's a standard way.
There are probably plenty of, you know, people that depict how they think you should do penetration testing.
But, you know, the notion of, you know, from -- you know, looking at a -- a code -- like, an application or a network and seeing if it can be -- in the case of penetration testing intruded upon, I think that's what people think about when they think about pen testing.
Q. Okay. If we could just quickly look at paragraph 6 of your report --
A. Uh-huh.
Q. -- page 2 carrying over to page 3.
A. Repeat the location again?
Q. Sure.
It's page 2 to 3, paragraph 6 --

A. Uh-huh.
Q. -- the last sentence of paragraph 6, you say, "My teams also assisted our clients in conducting penetration testing in red team exercises both of which involved structured testing efforts to find flaws and vulnerabilities in IT defenses."
A. Correct.
Q. What do you mean by "structured testing efforts"?
A. You know, that -- you know, when we conduct, you know, penetration testing or network-based red teaming, that, you know, there is a structure to our conduct of that activity in terms of what -- what we will do, how -- how that will interact with the client network, procedures for, you know, starting the testing.
You know, notifying clients about the fact that it's occurring. You know, procedures for if their incident response team, you know, detects the testing, you know, how to handle that.
You know, structure in terms of the nature of the reporting that we would undergo, you know, we would provide at the end of, kind of, conducting either pen testing or red teaming.

You know, generally, that's what I'm referring to when I talk about structured testing.
Q. Okay. And what are the forms of penetration testing that you recommend to your clients?
A. Yeah, again, it -- it really is, you know, situation dependent, yeah. It's very much situation dependent.
Q. Based on the documents that you've reviewed, how does SolarWinds perform penetration testing?
A. You know, during their -- you know, software development process, is it -- a series of tools that are used, reports that are generated, you know, related to penetration testing. I mean, the FSRs in many cases document that.
Q. Are you aware of SolarWinds conducting -- having any external penetration testing conducted?
MR. TURNER: Objection to form.
External penetration testing of software or external penetration testing of their network?
BY MR. CARNEY:
Q. Of their software.

A. You know, I didn't analyze, you know, what -- I mean, yeah, I didn't analyze if they had external, you know, penetration testing of -- of software.
You know, again, they had a very robust process for, you know, pen testing, you know, in the -- you know, in the -- you know, the evidence I examined and the -- also the -- the leaders of SolarWinds testified that they were doing it.
Q. All right. I could show you in your report, but just tell me if this is wrong.
In paragraph 87, you say that, "Penetration testing of software is often done with the assistance of automated tools which can simulate various types of attack -- attacks."
Is that true?
A. In paragraph 87, you know -- let's see. Down in, like, paragraph -- paragraph (c), okay. Let me just take a quick read.
(Pause for reading/reviewing.)
A. So I think you read a portion of this, but maybe just restate.
Q. All right. So in paragraph 87, subparagraph (c) --

A. Uh-huh --
Q. -- on page 48 --
A. -- yes.
Q. -- you say in the second sentence, "As with vulnerability testing, penetration testing of software is often done with the assistance of automated tools which can simulate various types of attack."
A. Correct.
Q. Are there any other penetration testing activities that -- other than those that use automated tools that you're familiar with?
A. I mean, yes.
Q. And what are they?
A. You know, you could, you know, have -- and I have seen, you know, this executed, you know, that the pen tester could just use -- and, again, maybe this is a nuance in terms of automated tools, but not pen testing tools, the normal ability of a computer to interact with another computer and see if they can gain access to the tested -- you know, either application or computer.
So I wouldn't call that sort of activity automated tools.

THE VIDEOGRAPHER: The time right now is 6:29 p.m.
We are off the record.
(Whereupon, a recess was taken at 6:29 p.m.)
THE VIDEOGRAPHER: The time right now is 6:36 p.m.
We're back on the record.
MR. CARNEY: All right. Dr. Rattray, I have no further questions at this time. I want to thank you for your time today.
THE WITNESS: Thank you.
MR. CARNEY: It was nice to meet you.
EXAMINATION
BY MR. TURNER:
Q. Should be pretty brief.
So, Dr. Rattray, let's pick up where Mr. Carney had left off a little while ago.
He asked you about whether the terms "secure development lifecycle" is a term of art.
Do you remember that?
A. I do.
Q. And he asked you about whether it comes from Microsoft.
Do you remember that?

Q. All right. And just a second ago when we were talking about paragraph 6 --
A. Uh-huh.
Q. -- and your team conducting penetration testing, which involves structured testing --
A. Uh-huh.
Q. -- efforts, I'm just trying to understand, what's the specific structure that you follow?
A. As I talked about it, you know, the structure that I'm talking about there is structure around the process by which we do it. Mostly to ensure that the safety and -- of the client.
Again, our penetration testing tends to be network penetration testing. We actually don't do application-level penetration testing, which is what, you know, is at issue in the SolarWinds case.
MR. CARNEY: Okay. Could we take, like, two minutes.
MR. TURNER: Sure.
///
///

A. I do.
Q. I think what Mr. Carney was getting at -- and correct me if I'm wrong -- is that if SolarWinds uses the phrase "our secured development life cycle" --
A. Right.
Q. -- in its security statement, would that be understood in the industry to mean that it does everything that Microsoft includes in its SDL?
A. No, no.
MR. CARNEY: Objection. Leading.
BY MR. TURNER:
Q. And why not?
A. You know, "secure development lifecycle," you know, again, is a broad -- you know, broadly interpreted term. You know, generally means there are things that you should do in order to make sure security is baked into your software development.
You know, the term at the level of secure development lifecycle is that broad, and you know -- you know, is not pinned to any specific, you know, set of practices.
Q. And so in your experience, do

companies tend to do software -- excuse me, secure development lifecycle the same way, or do they take different approaches?
A. Yeah. There's many different approaches.
Q. And in your experience, is it possible to have a secure development lifecycle without having formal threat modeling?
A. Yes. You could say you're doing secure development, you know, in a lifecycle fashion without threat modeling.
Q. Your report in places relies on some documents that date back before the relevant period; is that right?
A. That's true.
Q. For example, I think we talked about you cited a chat containing a screenshot of the password policy settings from before the relevant period?
A. That's right.
Q. Why, in your view, did you believe that that was reliable evidence of SolarWinds's practice during the relevant period?
A. You know, first, that screenshot is -- you know, the type of direct evidence you're

looking for just, in general, when you're doing these sorts of assessments.
You know, they -- they say that they're -- you know, conducting enforcement and, you know, the mechanism by which they were doing that is the use of active directory to enforce strong passwords.
That particular artifact, you know, shows that that -- that statement that, you know, of how they were doing their practice is just directly true.
It just shows the practice in implementation.
You know, it also -- have evidence to -- you know, that demonstrates that that continued, you know, into the -- into the relevant period, both in terms of, you know, testimony and auditors also looking at that specific situation and showing that that -- that implementation of the -- you know, the password practices was in place during the relevant period.
Q. And with respect to the training slide that we looked at earlier --
A. Yes.
Q. -- the SolarWinds development

process --
A. Uh-huh.
Q. -- this was from before the relevant period, right?
A. That's correct.
Q. Why did you consider this to be relevant evidence as to SolarWinds's practices within the relevant period?
A. Again, we -- we know from this -- you know, both, again, statements of executives and the presence of artifacts in the relevant -- you know, in the relevant period, like the final security reviews, that, you know, the practices outlined in that deck, which appears to be a training deck, you know, extended, you know, into the relevant period.
But that -- that particular deck shows SolarWinds starting a process of doing Agile development, and ensuring security is part of their approach to Agile development.
Q. As early as --
(Simultaneous unreportable crosstalk occurs among parties.)
(Stenographer requests one speaker at a time.)

BY MR. TURNER:
Q. As early as 2015; is that right?
A. Yes. As earlier as 2015 and then, again, evidenced during the relevant period in execution of the things that were outlined that had started as early as 2015.
Q. Let's go way back to sort of the beginning of the deposition.
You were asked about whether you have any certifications in various cybersecurity areas --
A. Yes, I remember being asked.
(Simultaneous unreportable crosstalk occurs among parties.)
BY MR. TURNER:
Q. -- or from cybersecurity authorities.
Let me ask you: Are certifications seen as important in the cybersecurity field, in your experience?
MR. CARNEY: Objection. Vague.
THE WITNESS: You know, in general, especially for the type of activity I was conducting here in terms of, you know, assessments of the presence of processes, you know, they're not, you know, seen as sort of necessary or even

sometimes particularly relevant to one's expertise in order to conduct these processes.
BY MR. TURNER:
Q. And has any of your clients ever asked you for certifications before engaging you to conduct cybersecurity assessments?
A. No.
MR. TURNER: No further questions.
MR. CARNEY: Just one brief follow-up question.
EXAMINATION
BY MR. CARNEY:
Q. Mr. Turner had asked you about your reliance on evidence or documents from before the relevant period.
Do you recall that?
A. Yes.
Q. Okay. And so, for instance, he mentioned the slide deck relating to SDL.
Do you recall that?
A. I think -- I think it's development process. You know, I mean, it was in our discussion of SDL, but -- this slide deck --
Q. Yeah.
A. -- is I believe what we were talking

about -- I was talking about with Mr. Turner.
Q. Okay. And the fact that you relied on documents like the slide deck that predated the relevant period, does that mean you were unable to find equivalent documentation to that slide deck from during the relevant period?
A. No. I mean, it does not mean that. As I stated, the types of things that were, you know, begun, you know, in training starting in, you know, 2015 as outlined in this deck were evidenced by, you know -- you know, processes like we discussed at length like the final security review, which was definitely prevalent throughout the -- you know, the relevant period.
Q. But did you find an equivalent slide deck from the relevant period?
A. I didn't -- I'm not sure even why I would have looked for one. You know, the point was -- you know, at least in my assessment was to show that, you know, they had -- they had in place, you know, during the relevant period per the securities statement processes.
This deck shows they initiated those processes and other evidence, you know, shows that they -- you know, they were implementing those

processes during the relevant period.
Q. And then actually just one more.
The folks that work for you at Next Peak, that, for instance, do penetration testing, did they have the certifications that Mr. Turner was asking you about?
MR. TURNER: Object to form.
THE WITNESS: Yeah, for the pen testers?
BY MR. CARNEY:
Q. Yes.
A. You know, I actually don't know necessarily if they -- they have those certifications or not. I mean, I'm -- yeah, I don't know for certain whether they have them.
MR. CARNEY: All right. No further questions, sir, thank you.
THE WITNESS: All right.
MR. TURNER: None for me.
THE VIDEOGRAPHER: The time right now is 6:45 p.m.
We are off the record.
THE STENOGRAPHER: Mr. Turner, did you want a rough draft?
MR. TURNER: Yes, please.

THE STENOGRAPHER: And regular delivery on final?
MR. TURNER: Yeah, that's fine.
(Time noted: 6:46 p.m.)

REPORTER CERTIFICATE

I, the undersigned, do hereby certify:

That GREGORY RATTRAY was by me duly sworn in the within-entitled cause; that said deposition was taken at the time and place herein named; and that the deposition is a true record of the witness's testimony as reported by me, a disinterested person, and thereafter was transcribed.

I further certify that I am not interested in the outcome of the said action, nor connected with, nor related to any of the parties in said action, nor to their respective counsel.

IN WITNESS WHEREOF, I have hereunto set my hand this 25th day of February, 2025.

Signature: __Requested__Waived_X_Not Requested

____
JESSICA R. WAACK
Registered Diplomate Reporter
Certified Realtime Reporter
California Certified Realtime Reporter
New York Realtime Court Reporter
New York Association Court Reporter
Notary Public, State of New York
CCR-NJ (No. 30XI008238700) CSR-TX (No. 11958)
CCR-WA (No. 21007264), CSR-CA (No. 14420)

313

ERRATA SHEET

Deposition of: GREGORY RATTRAY
Date taken: FEBRUARY 12, 2025
Case: SEC v. SOLARWINDS CORP., et al.
PAGE LINE
_____ _____ CHANGE: ______________________________
REASON: ______________________________
_____ _____ CHANGE: ______________________________
REASON: ______________________________
_____ _____ CHANGE: ______________________________
REASON: ______________________________
_____ _____ CHANGE: ______________________________
REASON: ______________________________
_____ _____ CHANGE: ______________________________
REASON: ______________________________
_____ _____ CHANGE: ______________________________
REASON: ______________________________
_____ _____ CHANGE: ______________________________
REASON: ______________________________
_____ _____ CHANGE: ______________________________
REASON: ______________________________
_____ _____ CHANGE: ______________________________
REASON: ______________________________
_____ _____ CHANGE: ______________________________
REASON: ______________________________
_____ _____ CHANGE: ______________________________
REASON: ______________________________
_____ _____ CHANGE: ______________________________
REASON: ______________________________
_____ _____ CHANGE: ______________________________
REASON: ______________________________
Signed____________________________
Dated____________________________

315

CERTIFICATE OF WITNESS

I, GREGORY RATTRAY, do hereby declare under penalty of perjury that I have read the entire foregoing transcript of my deposition testimony, or the same has been read to me, and certify that it is a true, correct and complete transcript of my testimony given on February 12, 2025, save and except for changes and/or corrections, if any, as indicated by me on the attached Errata Sheet, with the understanding that I offer these changes and/or corrections as if still under oath.

_____ I have made corrections to my deposition.
_____ I have NOT made any changes to my deposition.

Signed: ____________________________
GREGORY RATTRAY

Dated this ________ day of ______________ of 20____.

314

B

F

S

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 1:23-cv-09518-PAE

Notice of Errata – Deposition of Gregory Rattray (February 12, 2025)

I, the undersigned, do hereby declare that I have read the deposition transcript of Gregory Rattray dated February 12, 2025 and that to the best of my knowledge, said testimony is true and accurate, with the exception of the following changes listed below:

Pages and Line(s)	Change		Reason
	From	To	
14:22	information security, but	Information security field, but	Clarification
17:4-6	I helped with the formulation of the nation cybersecurity strategy	I helped with the formulation of the nation's cybersecurity strategy	Typographical error
17:9	Designed different programs	I designed different programs	Typographical error
[various][1]	security statement	Security Statement	Typographical error

[1] 23:1; 23:19; 74:19; 74:24; 75:21; 119:7; 121:18; 121:20; 129:18; 130:1; 139:25; 142:7; 151:5; 151:7; 151:10; 152:18; 153:9; 153:12; 153:17; 153:23; 156:9; 158:10; 175:6; 187:13; 187:24; 188:6; 188:7; 188:11; 194:7; 196:24; 207:12; 212:10; 212:24; 220:6; 220:10; 220:14; 221:10;

Pages and Line(s)	Change		Reason
	From	To	
26:11-12	I've conducted numerous assessments of companies, cybersecurity postures, control structures.	I've conducted numerous assessments of companies' cybersecurity postures and control structures.	Typographical error
28:8	operational	operationally	Typographical error
31:22	mostly a process,	mostly a process of,	Typographical error
32:18	do I do coding, I don't do coding	do I do coding?; I don't do coding	Clarification
34:15	In basically the idea	It's basically the idea	Typographical error
34:20	I've been the -- many person	I've been the main person	Typographical error
35:1	attune	attuned	Typographical error
54:10	I could reframe words	I could reframe the words	Typographical error
59:4	to the company	of the company	Clarification
65:9 66:2	Kline	Cline	Typographical error
68:9	in place at Insulet	were in place at Insulet	Clarification

221:15; 221:17; 246:2; 246:3; 255:11; 256:2; 256:8; 256:10; 257:4; 257:9; 258:3; 263:19; 263:20; 281:14; 281:16; 288:22; 291:24; 292:16; 292:20; 304:7.

Pages and Line(s)	Change		Reason
	From	To	
[various][2]	securities statement	Security Statement	Typographical error
72:10	I assume GAAP	I assume by GAAP	Clarification
74:5	controls or password.	controls or password policies.	Clarification
83:25	risumi	resume	Typographical error
84:13-14	the team that CISO is the senior director.	the team that the CISO is the senior director of.	Clarification
93:16	manage	managed	Typographical error
126:20	exclusion	conclusion	Typographical error
111:24	assessment company leadership	assessment to company leadership	Clarification
113:17–18	the digital real	the Digital Reality	Typographical error
134:11-12	This is a process that there's a lot of instances on,	This is a process that there's a lot of testimony on,	Typographical error
140:13-14	by the system access for forms and the user access request.	by the system access forms and the user access requests.	Typographical error
141:16-18	There are SARFs is one of the mechanisms that are used along with user access requests so -- as	SARFs are one of the mechanisms that are used along with user access requests, so that as	Clarification

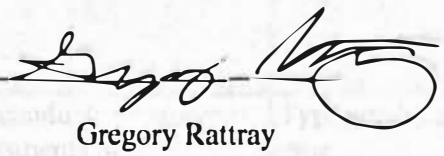
[2] 70:3; 73:15; 74:8; 75:6; 75:11; 102:10; 120:12; 120:23; 122:21; 123:11; 128:25; 135:8; 140:17; 142:3; 143:19; 144:25; 145:2; 153:14; 157:12; 158:24; 166:16; 170:9; 173:17; 180:21; 181:24; 188:14; 189:19; 189:24; 190:3; 191:5; 191:21; 192:24; 193:24; 194:14; 194:24; 206:21; 212:8; 229:24; 240:2; 244:19; 246:14; 250:17; 256:22; 258:18; 290:22; 291:11; 291:15; 310:22.

Pages and Line(s)	Change		Reason
	From	To	
144:19	auditors also looking at these	auditors are also looking at these	Clarification
150:5	But I was looking for	What I was looking for	Typographical error
151:25	documents demonstrate	documents that demonstrate	Clarification
155:11	SARF	SARFs	Typographical error
156:2	as we've assessed quite a bit	as we've discussed quite a bit	Typographical error
161:9	[indiscernable]	later	Typographical error
161:14	-- further attached form	-- attached form	Clarification
163:12	wouldn't appear as attachments	would appear as attachments	Typographical error
169:13	So I looked for these for presence of	So I looked through these for the presence of	Clarification
174:16	cleaning and pretty	clean and pretty	Typographical error
175:7	privileged	privilege	Typographical error
176:1	to read 18, 19	to read 118 and 119	Clarification
176:3	20	120	Clarification
195:24-25	And you can enforce where it's feasible to do so.	And you can only enforce where it's feasible to do so.	Clarification

Pages and Line(s)	Change		Reason
	From	To	
202:19-20	Mr. Colquitt's depositions and other technology leaders about how	Mr. Colquitt's deposition and other technology leaders' testimony about how	Clarification
208:2 209:15	checkmarks	Checkmarx	Typographical error
208:19 209:6 210:1 210:4	checkmark	Checkmarx	Typographical error
211:23	had the JIRA tickets	didn't have the JIRA tickets	Clarification
212:9	illumination	to illuminate	Clarification
214:23	where a security fit into it	where security fit into it	Clarification
218:24-25	using a password as a security incident	using a password was a security incident	Typographical error
232:9	SW-SEC-00166790	SW-SEC00166790	Typographical error
238:11-12	broadly you have threat modeling is about	broadly threat modeling is about	Clarification
244:9	if threat modeling	if they were threat modeling	Clarification
246:22-25	it's a strong process that there's no reason to believe that the things that are called for, you know, when they're present and the FSR, didn't happen.	it's a strong process and there's no reason to believe that the things that are called for, you know, when they're present in the FSR, didn't happen.	Clarification
248:14	me is a	me of a	Clarification

Pages and Line(s)	Change		Reason
	From	To	
257:11	haven't	have	Typographical error
288:16	Yeah, in the network security portion	THE WITNESS: Yeah, in the network security portion	Typographical error
294:5	device	advice	Typographical error

I declare under penalty of perjury that the foregoing is true and correct.

Date: March 20, 2025 Signed: 

Gregory Rattray